Red Hat Linux 8.0

Manual oficial de referencia de Red Hat Linux

Red Hat Linux 8.0: Manual oficial de referencia de Red Hat Linux
Copyright © 2002 por Red Hat, Inc.

Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Teléfono: +1 919 754 3700
Teléfono: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

rhl-rg(ES)-8.0-Print-RHI (2002-08-14T22:29-0400)
Copyright © 2002 por Red Hat, Inc. Este material se distribuye tan sólo bajo los términos y las condiciones establecidas en la Open Publication License, V1.0 o versión posterior (la última versión está disponible en http://www.opencontent.org/openpub/).
Los derechos de autor del propietario prohiben la distribución de versiones de este documento substancialmente modificadas sin un permiso explícito.
La distribución del producto o una copia del mismo en forma de libro con fines comerciales está prohibida a menos que se obtenga permiso previo del propietario de los derechos de autor.
Red Hat, Red Hat Network, el logo "Shadow Man" de Red Hat, RPM, Maximum RPM, el logo de RPM, Linux Library, PowerTools, Linux Undercover, RHmember, RHmember More, Rough Cuts, Rawhide y todas las marcas y logos basados en Red Hat son marcas registradas de Red Hat, Inc. en los Estados Unidos y otros países.
Linux es una marca registrada por Linus Torvalds.
Motif y UNIX son marchas registradas por The Open Group.
Intel y Pentium son marcas registradas de la Intel Corporation. Itanium y Celeron son marcas registradas de la Intel Corporation.
AMD, AMD Athlon, AMD Duron y AMD K6 son marcas registradas de la Advanced Micro Devices, Inc.
Netscape es una marca registrada de Netscape Communications Corporation en los Estados Unidos y otros países.
Windows es una marca registrada de Microsoft Corporation.
SSH y Secure Shell son marcas registradas de SSH Communications Security, Inc.
FireWire es una marca registrada de Apple Computer Corporation.
S/390 y zSeries son marcas registradas de la of International Business Machines Corporation.
La marca de GPG de la clave security@redhat.com es:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Tabla de contenidos

Introducción ix
1. Cambios realizados en este manual ix
2. Cómo encontrar la documentación apropiada. x
2.1. Documentación para usuarios principiantes de Linux x
2.2. Para los más experimentados xii
2.3. Documentación para gurús de Linux xii
3. Convenciones del documento xii
4. Uso del ratón xv
5. Copiar y pegar un texto con X xv
6. Y además xv
6.1. Necesitamos su opinión xvi
7. Regístrese para el soporte xvi
I. El sistema xvii
1. Estructura del sistema de ficheros 19
1.1. Porqué compartir una estructura común 19
1.2. Vista preliminar del estándar de jerarquía del sistema de ficheros (FHS) 19
1.3. Directorios especiales de Red Hat Linux 24
2. El sistema de ficheros `/proc` 25
2.1. Sistema de ficheros virtual 25
2.2. Ficheros de alto nivel en `/proc` 26
2.3. Directorios en `/proc` 40
2.4. Usar `sysctl` 56
2.5. Recursos adicionales 56
3. Proceso de arranque, inicio y cierre del sistema 59
3.1. Proceso de arranque 59
3.2. Vista detallada del proceso de arranque 59
3.3. Ejecutar programas en el tiempo de arranque 64
3.4. Diferencias en el proceso de arranque de otras arquitecturas 64
3.5. SysV Init 65
3.6. Niveles de ejecución Init 65
3.7. Directorio `/etc/sysconfig/` 67
3.8. Apagar 80
4. Gestores de arranque 83
4.1. Gestores de arranque y arquitectura del sistema 83
4.2. GRUB 83
4.3. Instalación de GRUB 84
4.4. Terminología de GRUB 85
4.5. Interfaces de GRUB 87
4.6. Comandos de GRUB 88
4.7. Fichero de configuración de menú de GRUB 89
4.8. LILO 90
4.9. Opciones en `/etc/lilo.conf` 92
4.10. Cambiar los niveles de ejecución en el tiempo de arranque 93
4.11. Recursos adicionales 94
5. Usuarios y grupos 95
5.1. Herramientas para la creación de usuarios y grupos 95
5.2. Usuarios estándar 95
5.3. Grupos estándar 97
5.4. Grupos de usuarios privados 99
5.5. Utilidades Shadow 100
6. El sistema X Window 103
6.1. El poder de X 103
6.2. XFree86 104
6.3. Entornos de escritorio y gestores de ventanas 108

6.4. Niveles de ejecución 110
6.5. Fuentes 112
6.6. Recursos adicionales 114
II. Seguridad 117
7. Pluggable Authentication Modules (PAM) 119
7.1. Las ventajas de PAM 119
7.2. Ficheros de configuración PAM 119
7.3. Módulos PAM 120
7.4. Los indicadores de control PAM 121
7.5. Rutas de módulos PAM 122
7.6. Argumentos PAM 122
7.7. Muestras de ficheros de configuración PAM 122
7.8. PAM y propiedad del dispositivo 124
7.9. Recursos adicionales 125
8. Los wrappers TCP y el comando `xinetd` 127
8.1. Qué son los wrappers TCP 127
8.2. Listas de control de acceso basadas en el nombre de la máquina 127
8.3. Control del acceso con el comando `xinetd` 131
8.4. Recursos adicionales 135
9. Protocolo SSH 137
9.1. Introducción 137
9.2. Secuencia de eventos de una conexión SSH 138
9.3. Capas de seguridad SSH 138
9.4. Ficheros de configuración OpenSSH 140
9.5. Más que una shell segura 141
9.6. Requisitos de SSH para conexiones remotas 143
10. Kerberos 145
10.1. ¿Por qué usar Kerberos? 145
10.2. ¿Por qué no usar Kerberos? 145
10.3. Terminología Kerberos 146
10.4. Modo en que funciona Kerberos 147
10.5. Kerberos y Pluggable Authentication Modules (PAM) 148
10.6. Configuración de un servidor Kerberos 5 148
10.7. Configuración de un cliente de Kerberos 5 150
10.8. Recursos adicionales 150
11. Tripwire 153
11.1. Cómo usar Tripwire 153
11.2. Instrucciones para la instalación de RPM 154
11.3. Personalización de Tripwire 155
11.4. Inicialización de la base de datos 158
11.5. Ejecución de un control de integridad 158
11.6. Verificación de los informes Tripwire 158
11.7. Actualización de la base de datos después de un control de integridad. 160
11.8. Actualización del fichero de política. 161
11.9. Actualización del fichero de configuración de Tripwire 163
11.10. Referencia de la localización del fichero Tripwire 163
11.11. Otros recursos 165

III. Servicios de red 167
12. Scripts de red 169
12.1. Ficheros de configuración de red 169
12.2. Ficheros de configuración de interfaz 169
12.3. Scripts de control de interfaz 174
12.4. Funciones de red 175
12.5. Recursos adicionales 175
13. Firewalls e `iptables` 177
13.1. Filtrado de paquetes 177
13.2. Diferencias entre `iptables` e `ipchains` 178
13.3. Opciones usadas en comandos `iptables` 179
13.4. Guardar información de `iptables` 186
13.5. Recursos adicionales 187
14. Servidor HTTP de Apache 189
14.1. Servidor HTTP de Apache 2.0 189
14.2. Migración de los ficheros de configuración de la versión 1.3 del Servidor HTTP de Apache 1.3 191
14.3. Después de la instalación 199
14.4. Arranque y apagado del comando `httpd` 200
14.5. Directivas de configuración en el fichero `httpd.conf` 200
14.6. Módulos predeterminados 217
14.7. Añadir módulos a su servidor 218
14.8. Utilización de máquinas virtuales 219
14.9. Recursos adicionales 220
15. Correo electrónico 223
15.1. Protocolos 223
15.2. Diferentes tipos de programas de correo electrónico 225
15.3. Sendmail 227
15.4. Fetchmail 231
15.5. Procmail 235
15.6. Seguridad 241
15.7. Recursos adicionales 242
16. Berkeley Internet Name Domain (BIND) 245
16.1. Introduccio´n al DNS y a BIND 245
16.2. Ficheros de configuración BIND 247
16.3. Utilización del comando `rndc` 257
16.4. Propidades avanzadas de BIND 259
16.5. Errores frecuentes que hay que evitar 261
16.6. Recursos adicionales 261
17. Network File System (NFS) 263
17.1. Metodología 263
17.2. Ficheros de configuración del servidor NFS 265
17.3. Ficheros de configuración de clientes NFS 267
17.4. Asegurar NFS 270
17.5. Recursos adicionales 271
18. Lightweight Directory Access Protocol (LDAP) 273
18.1. Razones por las que usar LDAP 273
18.2. Demonios y utilidades OpenLDAP 274
18.3. Terminología LDAP 276
18.4. Ficheros de configuración OpenLDAP 277
18.5. Vista preliminar de la configuración de OpenLDAP 279
18.6. Actualización de OpenLDAP a la versión 2.0 279
18.7. Configurar su sistema para la autenticación mediante OpenLDAP 279
18.8. Recursos adicionales 281

IV. Apéndices **283**
A. Parámetros generales y módulos 285
A.1. Especificación de parámetros de los módulos 285
A.2. Parámetros del módulo de CD-ROM 286
A.3. parámetros SCSI 288
A.4. Parámetros Ethernet 291
Índice **297**
Colophon **309**

Introducción

Bienvenido al *Manual oficial de referencia de Red Hat Linux*.

El *Manual oficial de referencia de Red Hat Linux* contiene la información necesaria sobre el sistema Red Hat Linux. Desde conceptos fundamentales, tales como la estructura del sistema de ficheros de Red Hat Linux, a la seguridad del sistema y el control de autenticación. Esperamos que este manual sea un recurso valioso para usted.

Este manual le ayudará a aprender más sobre el funcionamiento de su sistema Red Hat Linux. Podrá profundizar en los siguientes temas:

- Estructura del sistema de ficheros
- Proceso de arranque
- Sistema X Window
- Seguridad
- Servicios de red

1. Cambios realizados en este manual

Este manual ha sido reorganizado y actualizado con las últimas características de Red Hat Linux 8.0. Algunos cambios son los siguientes:

Nuevo capítulo de gestores de arranque

El capítulo de GRUB ha sido revisado e incluye LILO.

Un capítulo actualizado de Servidor HTTP de Apache

Ahora existe un manual para migrar de la versión 1.3 a la versión 2.0 del Servidor HTTP de Apache. También se ha actualizado la lista de las opciones de la configuración del servidor. Quisieramos dar las gracias a **Gary Benson** y **Joe Orton** por el gran trabajo que realizado en la elaboración del manual para la migración Servidor HTTP de Apache.

Capítulo actualizado de LDAP

Se ha reorganizado el capítulo del LDAP.

Capítulo actualizado de `iptables`

Se ha reorganizado el capítulo de los `iptables`.

Capítulo actualizado de Tripwire

Se ha reorganizado y revisado el capítulo de Tripwire (y tiene una graciosa nueva ilustración ;-).

Antes de leer este manual debería estar familiarizado con los contenidos del *Manual oficial de instalación de Red Hat Linux* relativos a la instalación, el *Manual oficial del principiante de Red Hat Linux* para conceptos básicos sobre Linux y el *Manual oficial de personalización de Red Hat Linux* para personalizar su sistema. El *Manual oficial de referencia de Red Hat Linux* contiene información sobre temas muy específicos que no afectan a todos los usuarios, dependiendo del uso que se le quiere dar al sistema Red Hat Linux.

Las versiones en HTML y en PDF de todos los manuales oficiales de Red Hat Linux están disponibles en línea en http://www.redhat.com/docs.

Nota

Aunque este manual contiene la información más actual, lea las Notas de última hora de Red Hat Linux si desea obtener más información. Se encuentran en el CD #1 de Red Hat Linux y en

`http://www.redhat.com/docs/manuals/linux`

2. Cómo encontrar la documentación apropiada

Necesita documentación apropiada a su nivel de experiencia con Linux. De lo contrario, se sentirá abrumado o no encontrará la información necesaria para responder a sus dudas. El *Manual oficial de referencia de Red Hat Linux* trata de aspectos más técnicos y de opciones de su sistema Red Hat Linux. Esta sección le ayudará a decidir, dependiendo de la información que necesite, si leer este manual u otros manuales Red Hat Linux, incluidos los recursos en línea.

Se pueden establecer tres categorías de personas que usan Red Hat Linux, e intentar ser más explícitos en cuanto a la documentación y fuentes de información necesarias. Puede empezar viendo el nivel de conocimiento que tiene:

Nuevo en Linux

Nunca ha usado el sistema operativo Linux o similar; o tiene muy pocos datos acerca de él. Tiene o no ha tenido experiencia usando otros sistemas operativos (como por ejemplo Windows). ¿Es ésta su situación? Si es así, por favor vuelva a la Sección 2.1.

Alguna experiencia con Linux

Ha instalado con éxito Linux y lo ha usado con anterioridad (pero no Red Hat Linux). O bien ha tenido experiencias equivalentes con otros sistemas operativos parecidos a Linux ¿Se encuentra usted entre este tipo de personas? Si es así,vuelva a leer la documentación Sección 2.2

Usuario avanzado

Ha instalado y usado Red Hat Linux con éxito en otras ocasiones. Si es así lea la Sección 2.3

2.1. Documentación para usuarios principiantes de Linux

Para alguien nuevo en Linux, la cantidad de información disponible sobre cada tema, como imprimir, arrancar el sistema o particionar su disco duro, puede ser abrumadora. Es conveniente que primero adquiera una buena base de conocimientos centrados entorno a cómo funciona Linux antes de entrar en temas más avanzados.

Su primer objetivo debería ser el de obtener documentación útil. De lo contrario se sentiría frustrado nada más empezar.

Trate de adquirir el siguiente tipo de documentación:

- *Una breve historia de Linux* — Muchos aspectos de Linux están ligados a precedentes históricos. Un poco de cultura sobre Linux puede ser útil a la hora de solventar problemas potenciales antes de que surjan.
- *Explicación acerca de cómo funciona Linux* — Aunque no es necesario profundizar en la mayoría de los aspectos del kernel Linux, es conveniente saber algo sobre cómo ha surgido Linux. Puede

ser especialmente importante si está trabajando con otros sistemas operativos, ya que algunas de las suposiciones que tiene sobre cómo funcionan los ordenadores pueden no cumplirse en Linux.

- *Vista preliminar a un comando de introducción (con ejemplos)* — Probablemente esto es lo más importante a buscar en la documentación linux. La filosofía de Linux es que es mejor usar pequeños comandos conectados de diferentes modos, que utilizar pocos comandos amplios (y complejos) que hagan todo el trabajo por si mismos. Sin algunos ejemplos que ilustren el acercamiento a Linux para hacer cosas, se puede sentir intimidado por el gran número de comandos disponibles en el sistema Red Hat Linux.

  Tenga en cuenta que no tiene que memorizar todos los comandos Linux. Existen diversas técnicas para ayudarle a encontrar el comando específico que necesita para realizar un tarea determinada. Tan sólo necesita saber el modo en que Linux funciona, lo que necesita llevar a cabo y cómo acceder a la herramienta que le dará las instrucciones exactas para ejecutar el comando.

El *Manual oficial de instalación de Red Hat Linux* constituye una referencia excelente de ayuda para instalar y configurar con éxito su sistema Red Hat Linux. El *Manual oficial del principiante de Red Hat Linux* cubre la historia de Linux, los comandos de sistema básicos, GNOME, KDE, RPM y otros muchos conceptos fundamentales. Debería empezar con estos dos libros y usarlos para conseguir una base de conocimiento sobre su sistema Red Hat Linux. Verá como después los conceptos más complicados empezarán a tener sentido, una vez que tenga las conceptos básicos claros.

A parte de leer los manuales Red Hat Linux, existen otras fuentes excelentes de documentación disponibles por poco dinero o gratis.

2.1.1. Introducción a sitios Web Linux

- http://www.redhat.com — en el sitio Web, podrá encontrar enlaces del proyecto de documentación Linux (LDP), versiones en línea de las FAQs (preguntas y respuestas más frecuentes), una base de datos que puede ayudarle en la búsqueda de grupos de usuarios Linux cercanos a usted, información técnica en la base de conocimientos de soporte de Red Hat y mucho más.
- http://www.linuxheadquarters.com — El sitio Web de la sede central de Linux le ofrece guías fáciles para una variedad de tareas Linux.

2.1.2. Introducción a los grupos de noticias de Linux

Puede participar en los grupos de noticias viendo las conversaciones de otros intentando solventar problemas, o bien puede participar activamente preguntando y contestando. Los usuarios experimentados de Linux le serán de una gran ayuda — especialmente si sus preguntas van a parar al punto de reunión justo. Si no tiene acceso a una aplicación de lector de noticias, puede acceder a esta información vía web en http://www.deja.com. Existen docenas de grupos de noticias relacionados con Linux entre las que se incluyen:

- linux.help — Un buen lugar donde encontrar ayuda de compañeros usuarios de Linux.
- linux.redhat — Este newsgroup cubre aspectos específicos a Red Hat Linux.
- linux.redhat.install — Para preguntas sobre instalación o para ver cómo otros han resuelto problemas similares.
- linux.redhat.misc — Preguntas o peticiones de ayuda que no encajan en ninguna de las categorías tradicionales.
- linux.redhat.rpm — Sitio donde dirigirse si tiene problemas con el uso de **RPM** para conseguir algún propósito en particular.

2.1.3. Libros sobre Linux

- *Red Hat Linux for Dummies, 2ª edición* de Jon "maddog" Hall; IDG
- *Special Edition Using Red Hat Linux* de Alan Simpson, John Ray y Neal Jamison; Que
- *Running Linux* de Matt Welsh y Lar Kaufman; O'Reilly & Associates
- *Red Hat Linux 7 Unleashed* de William Ball y David Pitts; Sams

Los libros aquí sugeridos constituyen fuentes excelentes de información para un conocimiento básico del sistema Red Hat Linux. Para una información más detallada sobre los diversos temas que aparecerán a través del libro, muchos de los capítulos listan títulos de libros específicos, habitualmente en la parte de *Recursos adicionales*.

2.2. Para los más experimentados

Si ha utilizado otras distribuciones Linux, tendrá un dominio básico de los comandos usados más frecuentemente. Puede que haya instalado su propio sistema Linux e incluso haya descargado y creado software que ha encontrado en Internet. Después de instalar Linux, no obstante, los puntos sobre configuración pueden ser confusos.

El *Manual oficial de personalización de Red Hat Linux* está diseñado para ayudar a explicar los diversos modos en que su sistema puede ser configurado. Utilice este manual para aprender las opciones de configuración y cómo ponerlas en práctica.

Cuando instale software que no aparezca en el *Manual oficial de personalización de Red Hat Linux*, le será útil ver lo que otra gente en las mismas circunstancias ha hecho. Los documentos HOWTO del LDP (proyecto de documentación de Linux), disponibles en http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html, documentan aspectos particulares de Linux, desde cambios del kernel hasta el uso de Linux en una estación de trabajo "radio amateur".

2.3. Documentación para gurús de Linux

Si es un usario Red Hat Linux desde hace tiempo, sabrá probablemente que uno de los mejores modos para entender un programa en particular es leyendo su código fuente y/o sus archivos de configuración. Una gran ventaja de Red Hat Linux es la disponibilidad total del código fuente.

Obviamente, no todo el mundo es programador de C, por lo que el código fuente no le puede ser de ayuda. Sin embargo, si tiene los conocimientos y la habilidad necesarios para leerlo, el código fuente alberga todas las respuestas.

3. Convenciones del documento

Cuando lea este manual, verá que algunas palabras están representadas en fuentes, tipos de letra, tamaño y peso diferentes. Esta forma de evidenciar es sistemática; se representan diferentes palabras con el mismo estilo para indicar su pertenencia a una categoría específica. A continuación tiene una lista de los tipos de palabras representados de una manera determinada:

`comando`

Los comandos en Linux (y otros sistemas operativos) se representan de esta manera. Este estilo le indica que puede escribir la palabra o frase en la línea de comandos y pulsar [Intro] para aplicar

el comando. A veces un comando contiene palabras que aparecerían con un estilo diferente si fueran solas (p.e, nombres de ficheros). En estos casos, se las considera como parte del comando, de manera que toda la frase aparece como un comando. Por ejemplo:

Utilice el comando `cat testfile` para ver el contenido de un fichero, llamado `testfile`, en el directorio actual.

`nombre del fichero`

Los nombres de ficheros, nombres de directorios, rutas y nombres de rutas y paquetes RPM aparecen siempre en este modo. Este estilo indica que un fichero o directorio en particular existe con ese nombre en su sistema Red Hat Linux. Ejemplos:

El fichero `.bashrc` en su directorio principal contiene definiciones de la shell de bash y alias para su propio uso.

El fichero `/etc/fstab` contiene información sobre diferentes dispositivos del sistema y sistemas de ficheros.

Instale el RPM `webalizer` si quiere utilizar un programa de análisis del fichero de registro del servidor Web.

aplicación

Este estilo indica que el programa nombrado es una aplicación para un usuario final (opuesto a software del sistema). Por ejemplo:

Use **Mozilla** para navegar por la Web.

[tecla]

Una tecla del teclado aparece en el siguiente estilo. Por ejemplo:

Para utilizar [Tab], introduzca un carácter y pulse la tecla [Tab]. Aparecerá una lista de ficheros en el directorio que empiezan con esa letra. Su terminal visualizará la lista de ficheros en el directorio que empieza con esa letra.

[Tecla]-[combinación]

Una combinación de teclas aparece de la siguiente manera. Por ejemplo:

La combinación de teclas [Ctrl]-[Alt]-[Backspace] le hará salir de la sesión gráfica y volver a la pantalla gráfica de login o a la consola.

texto de una interfaz gráfica (GUI)

Un título, palabra o frase dentro de una pantalla o ventana de interfaz gráfica GUI aparecerá de la siguiente manera. La finalidad del texto escrito en este estilo es la de identificar una pantalla GUI o un elemento e una pantalla GUI en particular (p.e, un texto relacionado con una casilla de verificación o un campo). Ejemplos:

Seleccione la casilla de verificación **Pedir contraseña** si quiere que su salvapantallas pida una contraseña antes de terminar.

nivel superior de un menú en una pantalla o ventana GUI

Cuando vea una palabra con este estilo, significa que la palabra está en el nivel superior de un menú desplegable. Si pulse sobre la palabra en la pantalla GUI, aparecerá el resto del menú. Por ejemplo:

Bajo **Fichero** en una terminal de GNOME verá los siguientes elementos en el menú: opción **Nueva pestaña** que le permite abrir múltiples intérpretes de comandos de la shell en la misma ventana.

Si tiene que escribir una secuencia de comandos desde un menú GUI, aparecerán como en el siguiente ejemplo:

Vaya a **Botón del menú principal** (en el Panel) => **Programación** => **Emacs** para iniciar el editor de textos **Emacs**.

botón en una pantalla o ventana GUI

Este estilo indica que el texto se encuentra en un botón que se pulse en una pantalla GUI. Por ejemplo:

Pulse el botón **Anterior** para volver a la última página Web que haya visitado.

`salida de pantalla`

Cuando vea el texto en este estilo, significa que verá una salida de texto en la línea de comandos. Verá respuestas a comados que haya escrito, mensajes de error e intérpretes de comandos para la entrada de datos durante los scripts o programas mostrados de esta manera. Por ejemplo:

Utilice `ls` para visualizar los contenidos de un directorio:

```
$ ls
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

La salida de pantalla que le devuelvan como respuesta al comando (en este caso, el contenido del directorio) se mostrará en este estilo.

`intérprete de comandos`

El intérprete de comandos es el modo en el que el ordenador le indica que está preparado para que usted introduzca datos, aparecerá con el siguiente estilo. Ejemplos:

```
$
#
[stephen@maturin stephen]$
leopard login:
```

`entrada del usuario`

El texto que el usuario tiene que escribir, ya sea en la línea de comandos o en una casilla de texto de una pantalla GUI, se visualizará en este estilo. En el siguiente ejemplo, **`text`** se visualiza en este estilo:

Para arrancar su sistema en modo texto de su programa de instalación, necesitará escribir en el comando **`text`** en el intérprete de comandos `boot:`.

Adicionalmente, usamos diferentes tipos de estrategias para llamar su atención para determinados tipos de información. Dependiendo de lo importante que esta información sea para su sistema, estos elementos serán marcados como nota, atención o aviso. Por ejemplo:

Nota

Recuerde que Linux es sensible a mayúsculas y minúsculas. En otras palabras, rosa no es lo mismo que ROSA o rOsA.

Sugerencia

El directorio `/usr/share/doc` contiene documentación adicional para paquetes instalados en su sistema.

Importante

Si modifica el fichero de configuración DHCP, los cambios no surtirán efecto hasta que el demonio DHCP se reinicie.

Atención

No lleve a cabo tareas rutinarias como root — utilice una cuenta de usuario normal a menos que necesite usar una cuenta de usuario para administrar su sistema.

Aviso

Si escoge no particionar de forma manual, una instalación de tipo servidor borrará todas las particiones ya existentes en los discos duros instalados. No escoja este tipo de instalación a menos que esté seguro de que no desea guardar los datos.

4. Uso del ratón

Red Hat Linux está diseñado para utilizar un ratón de tres botones. Si tiene un ratón de dos botones, debería haber seleccionado la emulación de tres botones durante el proceso de instalación. Si pulsa los dos botones a la vez, estará emulando el tercer botón, el del medio.

Si se le indica que pulse un elemento con el ratón, se da por descontado que nos referimos al botón izquierdo. Si necesita utilizar el botón del medio o el de la derecha, le será indicado explícitamente. (Esto será justamente lo contrario si ha configurado su ratón para que sea usado por una persona zurda.)

La frase "arrastrar y soltar" le debería ser familiar. Si se le indica que arrastre y suelte un elemento en su escritorio gráfico, haga click en el elemento y mantentga el botón del ratón pulsado. Mientras que lo mantiene pulsado, suelte el elemento moviendo el ratón a una nueva ubicación, dejando de presionar el botón para soltar el elemento.

5. Copiar y pegar un texto con X

Copiar y pegar un texto es fácil mediante el uso del ratón y del sistema X Window. Para copiar un texto, sencillamente haga click con el ratón y arrástrelo a lo largo del texto para evidenciarlo. Para pegar el texto en algún otro sitio, pulse el botón central del ratón en el hueco en el que quiere copiar el texto.

6. Y además...

El *Manual oficial de referencia de Red Hat Linux* forma parte del compromiso que Red Hat tiene con los usuarios al proporcionarles soporte útil y puntual. Las ediciones futuras contendrán más información sobre los cambios en la estructura del sistema y en la organización, nuevas y potentes herramientas de seguridad y otros recursos para ayudar a expandir la potencia del sistema Red Hat Linux — y su capacidad para usarlo.

Ahí es donde usted puede ayudar.

6.1. Necesitamos su opinión

Si encuentra algún error en el *Manual oficial de referencia de Red Hat Linux*, o si piensa que se necesitan hacer cambios, por favor mándenos su opinión a Bugzilla (http://bugzilla.redhat.com/bugzilla) contra el componente *rhl-rg*.

Asegúrese de mencionar el indentificador del manual:

```
rhl-rg(ES)-8.0-Print-RHI (2002-08-14T22:29-0400)
```

Así podremos saber de qué versión del manual se trata.

Si tiene alguna sugerencia, descríbanosla y si ha encotrado algún error indique la sección y parte del texto en el que se encuentre para facilitarnos la búsqueda.

7. Regístrese para el soporte

Si tiene una edición oficial de Red Hat Linux 8.0, recuerde que para beneficiarase de las ventajas que le corresponden como cliente de Red Hat, deberá registrarse.

Tiene derecho a usufruir las siguientes ventajas, dependiendo del producto oficial Red Hat Linux que haya comprado:

- Soporte oficial Red Hat — Obtenga ayuda con las preguntas de instalación del equipo de soporte de Red Hat, Inc..
- Red Hat Network — Actualice de forma sencilla los paquetes y reciba avisos de seguridad personalizadas para su sistema. Vaya a http://rhn.redhat.com para más detalles.
- *Under the Brim: Boletín oficial de Red Hat* — Obtenga mensualmente las últimas noticias e información sobre el producto directamente desde Red Hat.

Para registrarse vaya a http://www.redhat.com/apps/activate/. Encontrará el ID de su producto en una tarjeta negra, roja y blanca en la distribución oficial de Red Hat Linux.

Para leer más acerca del soporte técnico para Red Hat Linux remítase al apéndice *Obtener soporte técnico* en el apéndice del *Manual oficial de instalación de Red Hat Linux*.

¡ Buena suerte y gracias por haber escogido Red Hat Linux!

Equipo de documentación de Red Hat

El sistema

Capítulo 1.

Estructura del sistema de ficheros

1.1. Porqué compartir una estructura común

Una estructura de sistema de ficheros de un sistema operativo es el nivel más básico de organización. Casi siempre un sistema operativo interactúa con sus usuarios, aplicaciones y modelos de seguridad que dependen de la manera en que almacena los ficheros en un dispositivo de almacenamiento primario (normalmente una unidad de disco duro). Por varios motivos, es muy importante que los usuarios, así como los programas para la instalación y demás, sean capaces de referirse a unas pautas comunes para saber donde escribir y leer los ficheros binarios, la configuración, registro y otros ficheros.

Un sistema de ficheros se podría resumir en términos de dos categorías diferentes de ficheros:

- ficheros compartibles vs. no compartibles
- ficheros variables vs. estáticos

Los ficheros *compartibles* son aquéllos a los que se puede acceder desde varios hosts; mientras que los ficheros *no compartibles* no están disponibles a todos los hosts. Los ficheros *variables* pueden cambiar en cualquier momento sin una intervención del gestor de sistemas (activa o pasiva); los ficheros *estáticos*, tales como documentación y binarios, no cambian sin una actuación por parte del gestor de sistemas o de una agente que el gestor de sistemas haya escogido para realizar esta tarea.

El hecho de que estos ficheros sean vistos de esta manera se debe al tipo de permisos otorgados por el directorio que los sostiene. El modo en que el sistema operativo y sus usuarios necesitan utilizar los ficheros determina el directorio en el cual estos ficheros deberían estar ubicados, dependiendo de si el directorio está montado sólo en modo escritura o en modo lectura-escritura. El nivel más alto de esta organización es crucial, de la misma manera que el acceso a los directorios marcados puede ser restringido o se podrían manifestar problemas de seguridad si el nivel más alto se queda desorganizado o sin una estructura ampliamente utilizada.

No obstante, el hecho de tener simplemente una estructura no significa mucho a menos que ésta sea estándar. Las estructuras competitivas pueden causar más problemas de los que solucionan. Por esta razón, Red Hat ha escogido la estructura de sistema de ficheros y la ha extendido ligeramente para acomodar los ficheros especiales usados en Red Hat Linux.

1.2. Vista preliminar del estándar de jerarquía del sistema de ficheros (FHS)

Red Hat se ha comprometido a respetar el *Estándar de Jerarquía del Sistema Ficheros* (*FHS* del inglés Filesystem Hierarchy Standard), un documento de consenso que define los nombres y la situación de muchos ficheros y directorios. En el futuro se seguirá el estándar para asegurar la compatibilidad de Red Hat Linux

El documento que define el FHS es la referencia autorizada para cualquier sistema compatible FHS, sin embargo el estándar da pie a la extensibilidad de unas áreas o no define otras. En esta sección se proporciona un resumen del estándar y una descripción de aquellas partes del sistema de ficheros que no cubre el estándar.

El estándar completo está disponible en:

http://www.pathname.com/fhs

El cumplimiento del estándar significa varias cosas, los dos aspectos más importantes son la compatibilidad con otros sistemas que siguen el estándar y la capacidad de poder montar la partición `/usr` en modo sólo lectura pues contiene ejecutables comunes y no está pensado para ser alterada por los usuarios. Por este motivo, `/usr` puede ser montado directamente desde el CD-ROM o desde otro ordenador vía NFS en modo sólo lectura.

1.2.1. Organización de FHS

Los directorios y ficheros aquí anotados, son sólo un subconjunto de los especificados por el FHS. Véase la última versión del FHS para una descripción detallada.

1.2.1.1. Directorio `/dev`

El directorio `/dev` contiene archivos que representan dispositivos del sistema. Estos archivos son esenciales para el correcto funcionamiento del sistema.

1.2.1.2. Directorio `/etc`

El directorio`/etc` está reservado para archivos de configuración que afectan directamente a su ordenador. No deben colocarse ejecutables en `/etc`. Los ejecutables que antiguamente se colocaban en `/etc` deberían estar en `/sbin` o posiblemente en `/bin`.

Los directorios `X11` y `skel` deben ser subdirectorios de `/etc`:

```
/etc
  |- X11
  |- skel
```

El directorio `X11` es para archivos de configuración de X11 como `XF86Config`. El directorio `skel` es para archivos "esqueleto" (del inglés "skeleton") para usuarios, archivos que se utilizan para rellenar el directorio raíz de un usuario cuando éste es creado.

1.2.1.3. Directorio `/lib`

El directorio `/lib` debería contener sólo las librerías necesarias para ejecutar los binarios en `/bin` y `/sbin`. Estas imágenes de librerías compartidas son particularmente importantes para arrancar el sistema y ejecutar comandos en el sistema de ficheros de root.

1.2.1.4. Directorio `/mnt`

El directorio `/mnt` se refiere a sistemas de ficheros montados temporalmente, tales como CD-ROMs y disquetes.

1.2.1.5. Directorio `/opt`

El directorio `/opt` proporciona un área para almacenar habitualmente paquetes de software de una aplicación estática y amplia.

Para paquetes en los que se evite poner ficheros a través del sistema de ficheros, proporciona un sistema de organización predecible y lógico bajo el directorio de paquetes. Esto le aporta al gestor del sistema un modo sencillo de determinar el rol de cada fichero en un paquete particular.

Por ejemplo, si `sample` fuese el nombre de un paquete de software particular localizado en `/opt`, todos sus ficheros podrían ser emplazados en directorios dentro de `/opt/sample`, tales como `/opt/sample/bin` para binarios y `/opt/sample/man` para páginas de manual.

Los paquetes grandes que abarcan diferentes subpaquetes, cada uno de los cuales desempeñan una tarea especifica, también funcionan con `/opt`, aportando a este gran paquete un modo estándar de organizarse. De este modo, el paquete `sample` tendrá diferentes herramientas cada una de las cuales irá a sus subdirectorios, tales como `/opt/sample/tool1` y `/opt/sample/tool2`, cada uno de los cuales puede tener su propio `bin`, `man` y otros directorios similares.

1.2.1.6. El directorio `/proc`

El directorio `/proc` contiene "ficheros" especiales que o bien extraen información del kernel o bien la envían a éste.

Debido a la gran cantidad de datos que contiene el directorio `/proc` y a la gran cantidad de maneras utilizadas para comunicar con el kernel, se ha dedicado un capítulo entero a este tema. Para mayor información vea el Capítulo 2.

1.2.1.7. Directorio `/sbin`

El directorio `/sbin` es para ejecutables usados sólo por el usuario root. Los ejecutables en `/sbin` sólo se usan para arrancar y montar `/usr` y ejecutar operaciones de recuperación del sistema. El FHS dice:

> "`/sbin` contiene típicamente archivos esenciales para arrancar el sistema además de los binarios en `/bin`. Cualquier archivo ejecutado tras `/usr`, será montado (si no surge ningún problema) y ubicado en `/usr/sbin`. Los binarios de administración de sistema sólo local, deberían ser ubicados en `/usr/local/sbin`.

Los siguientes programas deberían encontrarse, al menos, en `/sbin`:

```
arp, clock,
getty, halt,
init, fdisk,
fsck.*, grub,
ifconfig, lilo,
mkfs.*, mkswap,
reboot, route,
shutdown, swapoff,
swapon, update
```

1.2.1.8. Directorio `/usr`

El directorio `/usr` es para archivos que puedan ser compartidos a través de todo el sitio. El directorio `/usr` habitualmente tiene su propia partición y debería ser montable en sólo lectura. Los siguientes directorios deberían ser subdirectorios `/usr`:

```
/usr
  |- bin
  |- dict
  |- etc
  |- games
  |- include
```

```
|- kerberos
|- lib
|- libexec
|- local
|- sbin
|- share
|- src
|- X11R6
```

El directorio `bin` contiene ejecutables, `doc` contiene páginas de documentación incompatibles con FHS, `etc` contiene ficheros de configuración de sistema, `games` es para juegos, `include` contiene los ficheros de cabecera C, `kerberos` contiene binarios y muchos más ficheros de Kerberos y `lib` contiene ficheros objeto y librerías que no están diseñadas para ser directamente utilizadas por usuarios o scripts de shell. El directorio `libexec` contiene programas de pequeña ayuda llamados por otros programas, `sbin` es para los binarios de administración del sistema (aquéllos que no pertenecen a `/sbin`), `share` contiene ficheros que no son de una arquitectura específica, `src` es para el código fuente y `X11R6` es para el sistema X Window (**XFree86** de Red Hat Linux).

1.2.1.9. Directorio `/usr/local`

El FHS dice:

> "La jerarquía `/usr/local` es para uso del gestor del sistema al instalar localmente el software. Necesita ser seguro para ser sobreescrito cuando el software del sistema es compartible entre un grupo de hosts, pero no se encuentra en `/usr`."

El directorio `/usr/local` es similar en estructura al directorio `/usr`. Tiene los siguientes subdirectorios, que son similares a los del directorio `/usr`:

```
/usr/local
       |- bin
       |- doc
       |- etc
       |- games
       |- include
       |- lib
       |- libexec
       |- sbin
       |- share
       |- src
```

1.2.1.10. Directorio `/var`

Ya que el FHS requiere que sea capaz de montar `/usr` en sólo lectura, cualquier programa que escriba ficheros log o que necesite los directorios `spool` o `lock` debería escribirlos en el directorio `/var`. El FHS constata que `/var` es para:

> "… ficheros de datos variables. Esto incluye ficheros spool, de administración, de registro y ficheros temporales."

Los siguientes directorios deberían ser subdirectorios de `/var`:

```
/var
```

```
 |- account
|- arpwatch
|- cache
|- crash
|- db
|- empty
|- ftp
|- gdm
|- kerberos
|- lib
|- local
|- lock
|- log
|- mail -> spool/mail
|- mailman
|- named
|- nis
|- opt
|- preserve
|- run
+- spool
     |- anacron
     |- at
     |- cron
     |- fax
     |- lpd
     |- mail
     |- mqueue
     |- news
     |- rwho
     |- samba
     |- slrnpull
     |- squid
     |- up2date
     |- uucp
     |- uucppublic
     |- vbox
     |- voice
|- tmp
|- tux
|- www
|- yp
```

Los ficheros log de sistema tales como `messages` y `lastlog` están en `/var/log`. El directorio `/var/lib/rpm` también contiene el sistema de datos RPM. Los ficheros lock van en `/var/lock`, habitualmente en directorios particulares para el programa en el uso del fichero. El directorio `/var/spool` tiene subdirectorios para varios sistemas que necesitan almacenar los ficheros de datos.

1.2.2. `/usr/local` en Red Hat Linux

En Red Hat Linux, el uso del directorio `/usr/local` es ligeramente diferente de lo especificado por FHS. El FHS establece que en `/usr/local` debería memorizarse el software que permanece seguro en las actualizacione de software de sistemas. Ya que las actualizaciones de sistemas de Red Hat se han realizado de forma segura con `/Herramienta de gestión de paquetes` y **rpm**, no necesita proteger archivos poniéndolos en `/usr/local`. Le recomendamos que use `/usr/local` para el software local de su máquina.

Por ejemplo, si usted ha montado `/usr` mediante sólo lectura de NFS desde un host local llamado `jake`. Si existe un paquete o programa que le gustaría instalar, pero no le es posible escribir en `jake` debería instalarlo bajo `/usr/local`. Si ha conseguido que el gestor de sistema de `jake` instale el programa en `/usr`, puede desinstalarlo desde `/usr/local`.

1.3. Directorios especiales de Red Hat Linux

Red Hat aumenta la estructura FHS para acomodar ficheros especiales que usa Red Hat Linux.

La mayor parte de los ficheros que pertenecen al *Administrador de paquetes de Red Hat* (*RPM*) se encuentran en el directorio `/var/lib/rpm/`. Para mayor información consulte el capítulo *Gestión de paquetes con RPM* en el *Manual oficial de personalización de Red Hat Linux*.

El directorio `/var/spool/up2date/` contiene los ficheros que usa la aplicación **Red Hat Update Agent** y que incluye información sobre el cabezal RPM. Esta usbicación se puede usar temporalmente para almacenar los RPMs descargados durante la actualización del sistema. Para mayor información sobre la Red Hat Network, vaya al sitio de Red Hat Network en https://rhn.redhat.com/.

Otra de las ubicaciones especiales (`/etc/sysconfig`) almacena la información de la configuración. Muchos scripts que se ejecutan al iniciar el sistema, usan los ficheros de este directorio. Sección 3.7.

Finalmente, otro directorio es el directorio `/initrd/`. Está vacío pero se usa como punto de montaj ecrítico durante el proceso de arranque.

Advertencia

No elimine el directorio `/initrd/` por ninguna razón . Si lo hace el sistema no podrá arrancar y aparecerán mensajes de error en el kernel.

redhat.

Capítulo 2.

El sistema de ficheros `/proc`

Las funciones primarias del kernel de Linux son controlar el acceso a los dispositivos físicos del ordenador y establecer cuándo y cómo deben de tener lugar la interacción entre estos dispositivos. El directorio `/proc` contiene ficheros virtuales visualizados que son ventanas del estado actual de la ejecución del kernel de Linux. Esto permite que el usuario acceda a un vasto compendio de información, proporcionándole de forma efectiva el punto de vista del kernel dentro del sistema. Además, el usuario puede utilizar el directorio `/proc` para comunicar cambios de configuración al kernel.

2.1. Sistema de ficheros virtual

En Linux, todo se guarda en ficheros. La mayoría de usuarios están familiarizados con los dos primeros tipos de ficheros, de texto y binarios. Sim embargo, el directorio `/proc` contiene ficheros que no son parte de ningún sistema de ficheros asociado a los discos duros, CD-ROM o cualquier otro dispositivo físico de almacenamiento conectado a su sistema (excepto la RAM). Mejor dicho, estos ficheros forman parte de un *sistema de ficheros virtual* habilitado a deshabilitado en el kernel de Linux cuando está compilado.

Los ficheros virtuales `/proc` poseen cualidades interesantes. En primer lugar, la mayoría de ellos tienen un tamaño de 0 bytes. Sin embargo, cuando se visualiza el fichero, éste puede contener una gran cantidad de información. Además, la mayoría de configuraciones del tiempo y las fechas reflejan el tiempo y fecha real, por lo que siempre están en constante cambio.

Algunos programas utilizan el sistema de ficheros `/proc` para descubrir los parámetros de un sistema y para que éstos puedan proporcionar mayor ejecución y ofrecer más características.

Además, un gestor de sistemas puede utilizar `/proc` como método sencillo de información de acceso sobre el estado del kernel, los atributos de las máquinas, los estados de los procesos individuales y mucho más. La mayoría de ficheros en este directorio, tales como `interrupts`, `meminfo`, `mounts` y `partitions` proporcionan una idea de lo que es un entorno de sistemas. Otros como `sistema de ficheros` y el directorio `/proc/sys/` dan información sobre la configuración del software.Para facilitar las cosas, los ficheros que contienen información sobre un tema parecido se agrupan en directorios virtuales y en subdirectorios, tales como `/proc/ide`.

2.1.1. Visualización de ficheros virtuales

Se puede acceder inmediatamente a una gran cantidad de información acerca del sistema, mediante el uso de los comandos `cat`, `more` o `less` en combinación con los ficheros en `/proc`. A continuación tiene un ejemplo dl tipo de CPU que tiene su ordenador:

```
processor : 0
vendor_id : AuthenticAMD
cpu family : 5
model  : 9
model name : AMD-K6(tm) 3D+ Processor
stepping : 1
cpu MHz  : 400.919
cache size : 256 KB
fdiv_bug : no
hlt_bug  : no
f00f_bug : no
coma_bug : no
fpu  : yes
```

```
fpu_exception : yes
cpuid level : 1
wp  : yes
flags  : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips : 799.53
```

Como puede ver, alguna información tiene sentido, mientras que otras áreas aparecen en un código extraño. Algunos de los ficheros `/proc` non tedrían sentido sin una leyenda con que guiarle. En muchos casos, las utilidades existen en el propio sistema, tales como `free` y `top`, que toman datos de estos ficheros y los visualizan de forma útil. Más ejemplos sobre esta aplicación son `apm`, `free` y `top`.

Nota

Algunos ficheros en `/proc` están configurados para que se puedan leer por el usuario root, de manera que deberá convertirse en usuario root antes de intentar leerlos.

2.1.2. Cambiar ficheros virtuales

En general, todos los ficheros que se encuentran en el directorio `/proc` solamente se pueden leer. Sin embargo, algunos se pueden usar para ajustar la configuración del kernel. Esto ocurre con los ficheros del subdirectorio `/proc/sys/`.

Para cambiar el valor de un fichero virtual use el comando `echo` y el símbolo > para introducir el nuevo valor en el fichero. De hecho, para cambiar el nombre del host escriba:

```
echo bob.subgenious.com > /proc/sys/kernel/hostname
```

Otros ficheros actúan como intercambiadores binarios. De hecho, si escribe `cat /proc/sys/net/ipv4/ip_forward`, verá el valor `0` o el valor `1`. El valor `0` indica que el kernel no está realizando el forwarding de los paquetes. Si usa el comando `echo` para cambiar el valor del fichero `ip_forward` a `1`, el kernel realizará el forwarding de los paquetes.

Nota

Otro comando que se usa para cambiara la configuración del subdirectorio `/proc/sys/` es `/sbin/sysctl`. Para mayor información consulte la Sección 2.4

Para consultar la lista de los ficheros de configuración del kernel disponibles en `/proc/sys/` vaya a Sección 2.3.8.

2.2. Ficheros de alto nivel en `/proc`

La siguiente lista expone algunos de los ficheros más comunes y útiles que se encuentran en el directorio `/proc`.

Nota

En la mayor parte de los casos, el contenido de los ficheros que aparecen en esta sección no será el mismo que el de su máquina. Esto se debe a que la mayor parte de la información pertenece al hardware en el que esté ejecutando RHL;.

2.2.1. /proc/apm

Este fichero proporciona inforamción acerca del estado de *Advanced Power Management (APM)* y las opciones en el sistema. Esta información viene usada por el kernel para proporcionar información para el comando `apm`.

La salida de este fichero en un sistema sin una bateria que está conectado a una fuente de energía AC se parece a:

```
1.16 1.2 0x03 0x01 0xff 0x80 -1% -1 ?
```

Al ejecutar un comando `apm -v` en estos sistemas resulta parecido a:

```
APM BIOS 1.2 (kernel driver 1.16)
AC on-line, no system battery
```

Para estos sistemas, `apm` será capaz de hacer más que poner una máquina en modo *standby*, comunmente se le conoce como "poner el sistema a dormir." El comando `apm` es mucho más útil en portátiles y otros sistemas Linux portables. Esto queda reflejado en los ficheros `/proc/apm`. Ésta es la salida de datos desde un fichero de muestra en un portátil que está ejecutando Linux, mientras que está conectado a una toma de corriente:

```
1.16 1.2 0x03 0x01 0x03 0x09 100% -1 ?
```

Cuando la misma máquina está desconectada de su fuente de energía y funciona con batería durante algunos minutos, el contenido del fichero `apm` cambiará:

```
1.16 1.2 0x03 0x00 0x00 0x01 99% 1792 min
```

En este estado, el comando `apm` cede información de lectura para estos datos:

```
APM BIOS 1.2 (kernel driver 1.16)
AC off-line, battery status high: 99% (1 day, 5:52)
```

2.2.2. /proc/cmdline

Este fichero muestra los parámetros pasados al kernel de Linux en el momento en que éste inicia. Ejemplo de fichero `/proc/cmdline`:

```
ro root=/dev/hda2
```

Los datos importantes contenidos en el fichero se segmentan de la siguiente manera: `ro` — significa que el kernel está cargado en modo sólo lectura. `root=/dev/hda2` — esta es la partición en la que se localiza el sistema de ficheros root.

2.2.3. /proc/cpuinfo

Este fichero cambia dependiendo del tipo de procesador de su sistema. La salida de datos es fácil de entender. Ejemplo:

```
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 5
model           : 9
model name      : AMD-K6(tm) 3D+ Processor
stepping        : 1
cpu MHz         : 400.919
cache size      : 256 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 1
wp              : yes
flags           : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips        : 799.53
```

- `procesador` — Proporciona un número de identificación para cada procesador. Si tan sólo posee un procesador, tan sólo verá un `0`.
- `cpu family` — Le da de forma autorizada el tipo de procesador que tiene en el sistema. Ponga el número delante del "86" para calcular el valor. Esto le servirá de ayuda si se está preguntando sobre el tipo de arquitectura de un sistema antiguo (686, 586, 486 or 386). Ya que los paquetes RPM están compilados de forma ocasional para arquitecturas particulares, este valor le indica qué paquete instalar en el sistema.
- `model name` — Le indica el nombre conocido del procesador, incluyendo el nombre de proyecto.
- `cpu MHz` — Le muestra la velocidad precisa en megahercios de ese procesador en particular (en milésimas).
- `cache size` — Le indica la cantidad de nivel 2 de la caché de memoria disponible en el procesador.
- `flags` — Define un número de cualidades diferentes del procesador, como la presencia de una unidad de coma flotante (FPU) y la habilidad para procesar instrucciones MMX.

2.2.4. /proc/devices

Este fichero visualiza los diversos caracteres y dispositivos de bloque actualmente configurados para el uso con el kernel. No incluye módulos que estén disponibles pero sin cargar en el kernel. El ejemplo de salida de datos de este fichero quedaría de la siguiente manera:

```
Character devices:
  1 mem
  2 pty
  3 ttyp
  4 ttyS
  5 cua
  7 vcs
```

```
 10 misc
 14 sound
 29 fb
 36 netlink
128 ptm
129 ptm
136 pts
137 pts
162 raw
254 iscsictl

Block devices:
  1 ramdisk
  2 fd
  3 ide0
  9 md
 22 ide1
```

La salida de datos desde `/proc/devices` incluye el mayor número y nombre de dispositivos y se divide en dos secciones:

Dispostivos de caracteres son parecidos a los *dispositivos de bloque*, a excepción de dos diferencias básicas.

En primer lugar, los dispositivos de bloque disponen de un buffer para peticiones, permitiendo que éstas sean tratadas por orden. Esto es muy práctico con dispositivos diseñados para guardar información, tales como discos duros, porque la habilidad de ordenar la información antes de escribirla en el dispositivo permite que ésta se almacecene de forma más eficiente. Los dispositivos de caracteres no necesitan dicha memoria.

En segundo lugar, los dispositivos de bloque pueden enviar y recibir información en bloques de un tamaño particular, que pueden ser configurada para cumplir los requisitos de un dispositivo en particular. Los dispositivos de caracteres envían datos en los bytes necesarios, sin un tamaño preconfigurado.

Puede encontrar más información sobre los dispositivos en `/usr/src/linux-2.4/Documentation/devices.txt`.

2.2.5. `/proc/dma`

Este fichero contiene una lista de los canales de acceso de memoria directos (DMA) ISA registrados en uso. Ejemplo de los ficheros `/proc/dma`:

```
 4: cascade
```

2.2.6. `/proc/execdomains`

Este fichero lista los dominios de ejecución soportados en la actualidad por el kernel de Linux junto con la gama de personalidades que soportan.

```
0-0   Linux           [kernel]
```

Piense en los *dominios de ejecución* como en una clase de "personalidad" de un sistema operativo en particular. Otros formatos binarios, como Solaris, UnixWare y FreeBSD pueden usarse con Linux. Al cambiar la personalidad de una tarea ejecutada bajo Linux, un programador puede cambiar el modo en el que el sistema operativo trata las llamadas del sistema particulares desde un binario. A excepción del dominio de ejecución `PER_LINUX`, el resto pueden ser implementados como módulos cargables de forma dinámica.

2.2.7. /proc/fb

Este fichero contiene una lista de dispositivos frame buffer, con el número del dispositivo frame buffer y el driver que lo controla. La salida de datos más común de `/proc/fb` para sistemas que contienen dispositivos de frame buffer es:

```
0 VESA VGA
```

2.2.8. /proc/filesystems

Este fichero visualiza una lista de los tipos del sistema de ficheros actuales soportados por el kernel. A continuación tiene un ejemplo de salida de datos desde un fichero `/proc/filesystems` del kernel genérico:

```
nodev rootfs
nodev bdev
nodev proc
nodev sockfs
nodev tmpfs
nodev shm
nodev pipefs
 ext2
nodev ramfs
 iso9660
nodev devpts
 ext3
nodev autofs
nodev binfmt_misc
```

La primera columna implica que el sistema de ficheros está montado en un dispositivo de bloque, con aquellos que contienen `nodev` en dicha columna implicando que éstos no están montados en un dispositivo de bloque. La segunda columna lista el nombre de los sistemas de ficheros soportados.

El comando `mount` utiliza la información para pasar por los posibles sisemtas de ficheros cuando uno no está especificado como un argumento.

2.2.9. /proc/interrupts

Este ficheros graba el número de interrupciones por IRQ en la arquitectura x86. Ejemplo de un fichero `interrupts` estándar:

```
           CPU0
  0:   80448940          XT-PIC  timer
  1:     174412          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          1          XT-PIC  rtc
 10:     410964          XT-PIC  eth0
 12:      60330          XT-PIC  PS/2 Mouse
 14:    1314121          XT-PIC  ide0
 15:    5195422          XT-PIC  ide1
NMI:          0
ERR:          0
```

Para una máquina multiprocesadora, el fichero aparecerá de forma diferente:

```
           CPU0       CPU1
```

```
  0: 1366814704          0          XT-PIC  timer
  1:        128        340    IO-APIC-edge  keyboard
  2:          0          0          XT-PIC  cascade
  8:          0          1    IO-APIC-edge  rtc
 12:       5323       5793    IO-APIC-edge  PS/2 Mouse
 13:          1          0          XT-PIC  fpu
 16:   11184294   15940594   IO-APIC-level  Intel EtherExpress Pro 10/100 Ethernet
 20:    8450043   11120093   IO-APIC-level  megaraid
 30:      10432      10722   IO-APIC-level  aic7xxx
 31:         23         22   IO-APIC-level  aic7xxx
NMI:          0
ERR:          0
```

La primera columna se refiere al número de IRQ. Cada CPU del sistema tiene su propia columna y su propio número de interrupciones por IRQ. La columna siguiente le indica el tipo de interrupción y la última contiene el nombre del dispositivo que está localizado en ese IRQ.

Cada uno de los tipos de interrupciones vistos en este fichero, específicos para el tipo de arquitectura, significan algo diferente. Los siguientes valores son comunes para las máquinas x86:

- `XT-PIC` — Interrupciones del ordenador AT antiguo que se han producido por un largo periodo de tiempo.
- `IO-APIC-edge` — Señal de voltaje de las transacciones interrumpidas desde abajo hasta arriba, creando una *edge*, en la que la interrupción `IO-APIC-level`, tan sólo se dan a partir de procesadores 586 y superiores.
- `IO-APIC-level` — Genera interrumpciones cuando suseñal de voltaje se alza hasta que la señal descende de nuevo.

2.2.10. `/proc/iomem`

Este fichero muestra el mapa actual de la memoria del sistema para los diversos dispositivos:

```
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-00291ba8 : Kernel code
  00291ba9-002e09cb : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  ea000000-ea00007f : tulip
ffff0000-ffffffff : reserved
```

La primera columna muestra los registros de memoria utilizados para cada uno de los diferentes tipos de memoria. La segunda columna indica el tipo de memoria de dichos registros. En particular, esta columna le mostrará qué registros de memoria son usados por el kernel den del sistema RAM o, si tiene puertos Ethernet múltiples en su NIC, los registros de memoria para cada puerto.

2.2.11. /proc/ioports

De forma similar a /proc/iomem, /proc/ioports proporciona una lista de puertos registrados actualmente utilizados para la comunicación de entrada y salida con un dispositivo. Este fichero puede ser muy largo y empezaría de la siguiente manera:

```
0000-001f : dma1
0020-003f : pic1
0040-005f : timer
0060-006f : keyboard
0070-007f : rtc
0080-008f : dma page reg
00a0-00bf : pic2
00c0-00df : dma2
00f0-00ff : fpu
0170-0177 : ide1
01f0-01f7 : ide0
02f8-02ff : serial(auto)
0376-0376 : ide1
03c0-03df : vga+
03f6-03f6 : ide0
03f8-03ff : serial(auto)
0cf8-0cff : PCI conf1
d000-dfff : PCI Bus #01
e000-e00f : VIA Technologies, Inc. Bus Master IDE
  e000-e007 : ide0
  e008-e00f : ide1
e800-e87f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  e800-e87f : tulip
```

La primera columna le indica la extensión de la dirección del puerto de entrada y salida para el dispositivo listado en la segunda columna.

2.2.12. /proc/isapnp

Este fichero lista las tarjetas *Plug and Play (PnP)* en espacios ISA del sistema. Esto es mucho más habitual con las tarjetas de sonido incluyendo, en ese caso, cualquier número de dispositivos. Un /proc/isapnp con una entrada Soundblaster vendría a ser de la siguiente manera:

```
Card 1 'CTL0070:Creative ViBRA16C PnP' PnP version 1.0 Product version 1.0
  Logical device 0 'CTL0001:Audio'
    Device is not active
    Active port 0x220,0x330,0x388
    Active IRQ 5 [0x2]
    Active DMA 1,5
    Resources 0
      Priority preferred
      Port 0x220-0x220, align 0x0, size 0x10, 16-bit address decoding
      Port 0x330-0x330, align 0x0, size 0x2, 16-bit address decoding
      Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
      IRQ 5 High-Edge
      DMA 1 8-bit byte-count compatible
      DMA 5 16-bit word-count compatible
      Alternate resources 0:1
        Priority acceptable
        Port 0x220-0x280, align 0x1f, size 0x10, 16-bit address decoding
        Port 0x300-0x330, align 0x2f, size 0x2, 16-bit address decoding
```

```
Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
IRQ 5,7,2/9,10 High-Edge
DMA 1,3 8-bit byte-count compatible
DMA 5,7 16-bit word-count compatible
```

Este fichero podría ser bastante largo dependiendo del número de dispositivos visualizados y de los requisitos o peticiones de recursos.

Cada tarjeta lista su nombre, número de versión PnP y versión del producto. Si el dispositivo está activo y configurado, este fichero revelará el puerto y los números de IRQ para el dispositivo. Además, para asegurar una mejor compatibilidad, la tarjeta especificará los valores `preferred` y `acceptable` para un número de parámetros diferentes. El objetivo es el de permitir que las tarjetas PNP funcionen en base a otra y evitar los problemas de IRQ y puertos.

2.2.13. /proc/kcore

Este fichero representa la memoria física del sistema y se almacena en el formato del fichero central. A diferencia de la mayoría de ficheros `/proc`, `kcore` muestra un tamaño. Este valor se da en bytes y es igual al tamaño de la memoria física (RAM) utilizada más 4KB.

Advertencia

Evite visualizar el fichero `kcore` en file `/proc`. Los contenidos de este fichero se saldrán del terminal. Si accidentalmente lo visualiza, pulse [Intro]-[C] para parar el proceso y luego escriba `reset` para volver a la línea de comandos del prompt en la estaba.

Sus contenidos están diseñados para que los examine un depurador, como por ejemplo `gdb`, el depurador de GNU.

2.2.14. /proc/kmsg

Este fichero se utiliza para mantener mensajes generados por el kernel y otros programas toman dichos mensajes, como por ejemplo `/sbin/klogd`.

2.2.15. /proc/ksyms

Este fichero contiene las definiciones del símbolo exportado del kernel usadas por las herramientas de módulos para enlazar y dinámicamente módulos cargables.

```
e003def4 speedo_debug [eepro100]
e003b04c eepro100_init [eepro100]
e00390c0 st_template [st]
e002104c RDINDOOR [megaraid]
e00210a4 callDone [megaraid]
e00226cc megaraid_detect [megaraid]
```

La segunda columna se refiere al nombre de una función del kernel y la primera columna lista la dirección de la memoria para dicha función. La última columna revela el nombre del módulo cargado para proporcionar dicha función.

2.2.16. /proc/loadavg

Este fichero ofrece una vista preliminar al promedio de carga o al uso del procesador, del mismo modo que le ofrece datos adicionales utilizados por `uptime` y otros comandos. Ejemplo:

```
0.20 0.18 0.12 1/80 11206
```

Las primeras tres columnas miden el uso de una CPU en los últimos periodos de 1, 5 y 10 minutos. La cuarta columna le muestra el número de procesos en ejecución en la actualidad y el número total de los mismos. La última columna visualiza el último proceso ID usado.

2.2.17. /proc/locks

Estos ficheros muestran los ficheros bloqueados en la actualidad por el kernel. El contenido de este fichero contiene datos internos de depuración y puede variar enormemente, dependiendo del uso del sistema. Ejemplo de fichero `locks` de un sistema ligeramente cargado:

```
1: FLOCK  ADVISORY  WRITE 807 03:05:308731 0 EOF c2a260c0 c025aa48 c2a26120
2: POSIX  ADVISORY  WRITE 708 03:05:308720 0 EOF c2a2611c c2a260c4 c025aa48
```

A cada bloqueo se le asigna un único núrmero al inicio de cada línea. La segunda columna se refiere a la clase de bloqueo utilizado; `FLOCK`, haciendo referencia al estilo antiguo de bloqueos de ficheros desde una llamada de sistema `flock` y `POSIX` que representa los bloqueos nuevos POSIX desde la llamada de sistema `lockf`.

La tercera columna puede tener dos valores. `ADVISORY` significa que el bloqueo no impide que otras personas puedan acceder a los datos; tan sólo previene de otros intentos de bloqueo. `MANDATORY` significa que mientras que dura el bloqueo no se permite ningún otro acceso a los datos. La cuarta columna muestra si el bloqueo permite al responsable del mismo el acceso a `READ` o acceso `WRITE` al fichero y la quinta muestra el ID del proceso de bloqueo.

La sesta columna muestra el ID del fichero bloqueado, en formato *`MAJOR-DEVICE`*`:`*`MINOR-DEVICE`*`:`*`INODE-NUMBER`*. La séptima muestra el inicio y el final de la región bloqueada del fichero. Las columnas restantes señalan las estructuras de los datos del kernel interno usadas para una depuración especializada y no hace falta tenerlas en cuenta.

2.2.18. /proc/mdstat

Este fichero contiene información actual sobre las configuración del disco múltiple, de RAID. Si su sistema no contiene dicha configuración, el fichero `mdstat` será parecido a:

```
Personalities :
read_ahead not set
unused devices: <none>
```

Si posee dispositivos `md` creados y en uso, podrá utilizar `mdstat` que le permitirá ver una fotografía de lo que está ocurriendo con sus dispositivos `md`*`X`*.

Este fichero `/proc/mdstat` un sistema con `md0` configurado como un dispositivo 1 de RAID que está resincronizando los discos en ese momento y se pueden ver el porcentaje completad y el tiempo restante estimado:

```
Personalities : [linear] [raid1]
read_ahead 1024 sectors
md0: active raid1 sda2[1] sdb2[0] 9940 blocks [2/2] [UU] resync=1% finish=12.3min
algorithm 2 [3/3] [UUU]
unused devices: <none>
```

2.2.19. /proc/meminfo

Éste es uno de los ficheros /proc más utilizados, ya que remiten mucha información importante sobre el uso actual de RAM en el sistema. Un sistema con 256MB de RAM y 384MB de espacio swap tendrá un fichero /proc/meminfo parecido al siguiente:

```
        total:    used:    free:  shared: buffers:  cached:
Mem:  261709824 253407232  8302592        0 120745984 48689152
Swap: 402997248     8192 402989056
MemTotal:       255576 kB
MemFree:          8108 kB
MemShared:           0 kB
Buffers:        117916 kB
Cached:          47548 kB
Active:         135300 kB
Inact_dirty:     29276 kB
Inact_clean:       888 kB
Inact_target:        0 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       255576 kB
LowFree:          8108 kB
SwapTotal:      393552 kB
SwapFree:       393544 kB
```

El comando top utiliza la mayoría de información. De hecho, la salida de datos del comando free es parecida, aparentemente, al contenido y estructura de meminfo. Si lee directamente meminfo conocerá muchos detalles sobre la memoria:

- Mem — Muestra el estado actual de RAM física en el sistema, incluyendo el uso en bytes de memoria total usada, libre, compartida, buffer y caché.
- Swap — Muestra la cantidad total de espacio swap libre y usado en bytes.
- MemTotal — Cantidad total de RAM física en kilo bytes.
- MemFree — Cantidad de RAM física, en kilobytes, sin utilizar por el sistema.
- MemShared — No se utiliza con 2.4 y kernels superiores pero se deja por motivos de compatibilidad con versiones del kernel precedentes.
- Buffers — Cantidad de RAM física, en kilobytes, usada para los ficheros de buffers.
- Cached — Cantidad de RAM física en kilobytes usada como memoria caché.
- Active — Cantidad total de buffer o memoria caché de página, en kilobytes, que está en uso activo.
- Inact_dirty — Cantidad total de buffer y páginas de la caché, en kilobytes, que podrían quedar libres.
- Inact_clean — Cantidad total de buffer y páginas de la caché en kilobytes que definitvamente están libres y disponibles.
- Inact_target — Cantidad de red de asignaciones por segundo, en kilobytes, con un promedio de un minuto.
- HighTotal y HighFree — Cantidad total de memoria libre, que no está implantada en el espacio del kernel. El valor HighTotal puede variar dependiendo del tipo de kernel utilizado.
- LowTotal y LowFree — Cantidad total de memoria libre implantada directamente en el espacio del kernel. El valor LowTotal puede cambiar dependiendo del tipo de kernel utilizado.
- SwapTotal — Cantidad total de swap disponible, en kilobytes.

- SwapFree — Cantidad total de swap libre, en kilobytes.

2.2.20. /proc/misc

Este fichero lista varios controladores registrados en el principal dispositivo diverso, que es el número 10:

```
135 rtc
  1 psaux
134 apm_bios
```

La primera columna es el número menor de cada dispositivo y la segunda le muestra el driver en uso.

2.2.21. /proc/modules

Este fichero visualiza una lista de todos los módulos han sido cargados por el sistema. Su contenido variará dependiendo de la configuración y uso de su sistema, pero debería organizarse de forma similar al siguiente ejemplo de salida de datos del fichero /proc/modules:

```
ide-cd                  27008   0 (autoclean)
cdrom                   28960   0 (autoclean) [ide-cd]
soundcore                4100   0 (autoclean)
agpgart                 31072   0 (unused)
binfmt_misc              5956   1
iscsi                   32672   0 (unused)
scsi_mod                94424   1 [iscsi]
autofs                  10628   0 (autoclean) (unused)
tulip                   48608   1
ext3                    60352   2
jbd                     39192   2 [ext3]
```

La primera columna contiene el nombre del módulo. La segunda se refiere al tamaño de memoria del módulo en bytes. La tercera le indica si el módulo está cargado (1) o descargado (0) en la actualidad. La última columna le indica si el módulo puede descargarse por si mismo automáticamente tras un periodo en el que no ha usado (autoclean) o si no se está utilizando (unused). Cualquier módulo con una línea que contenga un nombre listado entre corchetes ([o]) le indica que este módulo depende de que otro esté presente para que funcione.

2.2.22. /proc/mounts

Este fichero proporciona una lista rápida de todos los montajes en uso del sistema:

```
rootfs / rootfs rw 0 0
/dev/hda2 / ext3 rw 0 0
/proc /proc proc rw 0 0
/dev/hda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```

La salida de datos que encontramos se parece /etc/mtab, pero /proc/mount puede ser más actual.

La primera columna especifica el dispositivo que está montado y la segunda revela el punto de montaje. La tercera le indica el tipo de sistema de ficheros y la cuarta si está montado en modo sólo lectura

(ro) o sólo escritura (rw). La quinta y sexta columna son valores no válidos diseñados para hacer coincidir el formato usado en /etc/mtab.

2.2.23. /proc/mtrr

Este fichero se refiere a la memoria actual Memory Type Range Registers (MTRRs) en uso con el sistema. Si la arquitectura de su sistema soporta MTRRs, su mtrr será algo parecido a:

```
reg00: base=0x00000000 (   0MB), size=  64MB: write-back, count=1
```

Los MTRRs se usan con procesadores de tipo Intel P6 (Pentium Pro y superiores) para controlar el acceso del procesador a la capacidad de la memoria. Cuando utilice una tarjeta de vídeo en un PCI o un bus AGP, un fichero mtrr adecuadamente configurado puede incrementar la ejecución en un 150%.

La mayoría de las veces, este valor está configurado adecuadamente. Para más información sobre MTRRs y la configuración de este fichero de forma manual consulte http://web1.linuxhq.com/kernel/v2.3/doc/mtrr.txt.html.

2.2.24. /proc/partitions

La mayoría de la información no es relevante para los usuarios, a excepción de las siguientes líneas:

- major — Número principal del dispositivo con esta partición. El número principal en nuestro ejemplo (3) corresponde con el dispositivo ide0 en /proc/devices, permitiéndonos conocer el tipo de driver de dispositivo usado para interactuar con esa partición.
- minor — Número menor del dispositivo con esta partición. Separa las particiones en diferentes dispositivos físicos y los relaciona con el número al final del nombre de la partición.
- #blocks — Lista el número de bloques de disco físicos contenidos en una partición particular.
- name — Nombre de la partición.

2.2.25. /proc/pci

El fichero contiene una lista completa de cada dispositivo PCI de su sistema. Dependiendo del número de dispositivos PCI que posea, /proc/pci puede ser bastante largo. Ejemplo de este fichero en un sistema básico:

```
Bus  0, device   0, function  0:
  Host bridge: Intel Corporation 440BX/ZX - 82443BX/ZX Host bridge (rev 3).
    Master Capable.  Latency=64.
    Prefetchable 32 bit memory at 0xe4000000 [0xe7ffffff].
Bus  0, device   1, function  0:
  PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev 3).
    Master Capable.  Latency=64.  Min Gnt=128.
Bus  0, device   4, function  0:
  ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 2).
Bus  0, device   4, function  1:
  IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 1).
    Master Capable.  Latency=32.
    I/O at 0xd800 [0xd80f].
Bus  0, device   4, function  2:
  USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 1).
```

```
      IRQ 5.
      Master Capable.  Latency=32.
      I/O at 0xd400 [0xd41f].
  Bus  0, device   4, function  3:
    Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 2).
      IRQ 9.
  Bus  0, device   9, function  0:
    Ethernet controller: Lite-On Communications Inc LNE100TX (rev 33).
      IRQ 5.
      Master Capable.  Latency=32.
      I/O at 0xd000 [0xd0ff].
      Non-prefetchable 32 bit memory at 0xe3000000 [0xe30000ff].
  Bus  0, device  12, function  0:
    VGA compatible controller: S3 Inc. ViRGE/DX or /GX (rev 1).
      IRQ 11.
      Master Capable.  Latency=32.  Min Gnt=4.Max Lat=255.
      Non-prefetchable 32 bit memory at 0xdc000000 [0xdfffffff].
```

Esta salida de datos muestra una lista de todos los dispositivos PCI, en orden de bus, dispositivo y función. Además de proporcionar el nombre y versión del dispositivo, que va muy bien saber si no se acuerda de la marca de su tarjeta de interfaz de red, esta lista le proporciona información de IRQ detallada para que pueda dar con los problemas rápidamente.

Nota

Para mayor información escriba:

```
lspci -vb
```

2.2.26. /proc/slabinfo

Este fichero le da información sobre el uso de memoria a nivel slab. Los kernels de Linux superiores a 2.2 utilizan *slab pools* para gestionar la memoria superior al nivel de la página. Los objetos utilizados habitualmente, tienen sus propios slab pools. A continuación le mostramos una parte de un típico fichero `/proc/slabinfo` virtual:

```
slabinfo - version: 1.1
kmem_cache            64     68    112    2    2    1
nfs_write_data         0      0    384    0    0    1
nfs_read_data          0    160    384    0   16    1
nfs_page               0    200     96    0    5    1
ip_fib_hash           10    113     32    1    1    1
journal_head          51   7020     48    2   90    1
revoke_table           2    253     12    1    1    1
revoke_record          0      0     32    0    0    1
clip_arp_cache         0      0    128    0    0    1
ip_mrt_cache           0      0     96    0    0    1
```

Los valores en este fichero acontecen en el siguiente orden: nombre de la caché, nombre de objetos activos, nombre de objetos totales, tamaño del objeto, nombre de slabs activos (bloques) de los objetos, número total de slabs de los objetos y el número de páginas por slab.

Cabe remaracar que la palabra *activo* en este caso significa estar en uso. Un objeto activo es un objeto en uso y un slab activo es el que contiene cualquier objeto usado.

2.2.27. /proc/stat

Este fichero le aporta diferentes estadísticas sobre el sistema desde que fue reiniciado por última vez. El contenido de /proc/stat que puede ser muy largo, empieza de la siguiente manera:

```
cpu  1139111 3689 234449 84378914
cpu0 1139111 3689 234449 84378914
page 2675248 8567956
swap 10022 19226
intr 93326523 85756163 174412 0 3 3 0 6 0 1 0 428620 0 60330 0 1368304 5538681
disk_io: (3,0):(1408049,445601,5349480,962448,17135856)
ctxt 27269477
btime 886490134
processes 206458
```

Algunas de las estadísticas más populares incluyen:

- cpu — Mide el número de *jiffies* (1/100ths de un segundo) que el sistema ha estado en modo usuario, modo usuario con prioridad baja, modo del sistema y tarea inactiva respectivamente. El total de todas las CPUs se da al inicio y cada CPU individual se lista debajo con sus propias estadísticas.
- page — Número de páginas que el sistema ha cargado o suprimido del disco.
- swap — Número de páginas swap que el sistema ha introducido o sacado.
- intr — Número de interrupciones que ha experimentado el sistema.
- btime — Tiempo de arranque, medido por el número de segundos desde el 1 de enero de 1970, conocido con el nombre de *epoch*.

2.2.28. /proc/swaps

Este fichero mide el espacio swap y su uso. Para un sistema con tan sólo una partición de espacio swap, la salida de datos de /proc/swap será:

```
Filename   Type  Size Used Priority
/dev/hda6                       partition 136512 20024 -1
```

Mientras que alguna de esta información se puede encontrar en otros ficheros /proc, swap proporciona una instantánea rápida de cada nombre de fichero swap, tipo de espacio swap y el tamaño total usado (en kilobytes). La columna prioritaria es útil cuando múltiples ficheros swap están en uso y se prefieren algunos de ellos a otros, como si estuvieran en discos duros más rápidos. Cuanto más baja es la prioridad, más probable es que se use un fichero swap.

2.2.29. /proc/uptime

El fichero contiene información sobre el tiempo que lleva encendido el sistema desde el último reinicio. La salida de datos de /proc/uptime es mínima:

```
350735.47 234388.90
```

El primer número le indica el número total de segundos que el sistema ha estado en funcionamiento. El segundo indica cuánto de ese tiempo, también en segundos, la máquina ha estado inactiva.

2.2.30. /proc/version

Estos ficheros muestran las versiones del kernel de Linux y gcc, así como la versión de Red Hat Linux instalada en el sistema:

```
Linux version 2.4.18-0.40 (user@foo.redhat.com) (gcc version 2.96 20000731
(Red Hat Linux 7.2 2.96-102)) #1 Tue May 28 04:28:05 EdT 2002
```

Esta información se usa para diversos propósitos, incluyendo la aportación de datos de la versión en el intérprete de comandos de registro estándar.

2.3. Directorios en /proc

Grupos comunes de información referente al kernel agrupado en directorios y subdirectorios en /proc/.

2.3.1. Directorios de proceso

Cada directorio /proc/ contiene unos cuantos directorios nombrados con un número. Un listado de los mismos empezaría de la siguiente manera:

```
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1010
dr-xr-xr-x    3 xfs      xfs             0 Feb 13 01:28 1087
dr-xr-xr-x    3 daemon   daemon          0 Feb 13 01:28 1123
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 11307
dr-xr-xr-x    3 apache   apache          0 Feb 13 01:28 13660
dr-xr-xr-x    3 rpc      rpc             0 Feb 13 01:28 637
dr-xr-xr-x    3 rpcuser  rpcuser         0 Feb 13 01:28 666
```

A estos directorios se les llama *directorios de proceso*, ya que pueden hacer referencia a un ID de proceso y contener información específica para ese proceso. El propietario y grupo de cada directorio de proceso está configurado para que el usuario ejecute el proceso. Cuando se finaliza el proceso, el directorio del proceso /proc desaparece. Sin embargo, mientras que se está ejecutando el proceso, una gran cantidad de información específica a ese proceso está contenida en varios ficheros del directorio de procesos.

Cada uno de los directorios de procesos contiene los siguientes ficheros:

- cmdline — Contiene los argumentos de la línea de comandos que iniciaron el proceso. El fichero de salida de datos de cmdline para el proceso sshd sería parecido a:
  ```
  /usr/sbin/sshd
  ```
- cpu — Proporciona información específica sobre el uso de cada uno de las CPUs del sistema. Un proceso que se ejecuta en un sistema CPU dual produciría la siguiente salida de datos:
  ```
  cpu  11 3
  cpu0 0 0
  cpu1 11 3
  ```
- cwd — Enlace al directorio actual en funcionamiento para el proceso.
- environ — Le da una lista de variables de entorno para el proceso. La variable de entorno en mayúsculas y el valor en minúsculas.
- exe — Enlace al ejecutable de este proceso.

- `fd` — Directorio que contiene todos los descriptores de ficheros par un proceso en particular. Vienen dados en enlaces numerados:

```
total 0
lrwx------    1 root     root           64 May  8 11:31 0 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 1 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 2 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 3 -> /dev/ptmx
lrwx------    1 root     root           64 May  8 11:31 4 -> socket:[7774817]
lrwx------    1 root     root           64 May  8 11:31 5 -> /dev/ptmx
lrwx------    1 root     root           64 May  8 11:31 6 -> socket:[7774829]
lrwx------    1 root     root           64 May  8 11:31 7 -> /dev/ptmx
[root@bleach /]#
```

- `maps` — Contiene mapas de memoria para los diversos ejecutables y ficheros de librería asociados con este proceso. Este fichero puede ser bastante largo, dependiendo de la complejidad del proceso. Una muestra de la salida de datos desde el proceso `sshd` empezaría de la siguiente manera:

```
08048000-08086000 r-xp 00000000 03:03 391479     /usr/sbin/sshd
08086000-08088000 rw-p 0003e000 03:03 391479     /usr/sbin/sshd
08088000-08095000 rwxp 00000000 00:00 0
40000000-40013000 r-xp 00000000 03:03 293205     /lib/ld-2.2.5.so
40013000-40014000 rw-p 00013000 03:03 293205     /lib/ld-2.2.5.so
40031000-40038000 r-xp 00000000 03:03 293282     /lib/libpam.so.0.75
40038000-40039000 rw-p 00006000 03:03 293282     /lib/libpam.so.0.75
40039000-4003a000 rw-p 00000000 00:00 0
4003a000-4003c000 r-xp 00000000 03:03 293218     /lib/libdl-2.2.5.so
4003c000-4003d000 rw-p 00001000 03:03 293218     /lib/libdl-2.2.5.so
```

- `mem` — Memoria del proceso.
- `root` — Enlace al directorio root del proceso.
- `stat` — Estado del proceso.
- `statm` — Estado de la memoria en uso por el proceso. Ejemplo de ficheros `statm`:

```
263 210 210 5 0 205 0
```

  Las siete columnas se relacionan a diferentes estadísticas de memoria para el proceso. Dependiendo de como se visualizan, de derecha a izquierda, remiten diferentes aspectos de la memoria utilizada:

  1. Tamaño total del programa, en kilobytes
  2. Tamaño de porciones de memoria, en kilobytes
  3. Número de páginas compartidas
  4. Número de páginas en código
  5. Número de páginas de datos/grupos
  6. Número de páginas de librería
  7. Número de páginas sucias

- `status` — Proporciona el estado del proceso en una forma mucho más legible que `stat` o `statm`. Ejemplo de salida de datos de `sshd`:

```
Name: sshd
State: S (sleeping)
Tgid: 797
Pid: 797
PPid: 1
TracerPid: 0
Uid: 0 0 0 0
Gid: 0 0 0 0
FDSize: 32
```

```
Groups:
VmSize:     3072 kB
VmLck:         0 kB
VmRSS:      840 kB
VmData:      104 kB
VmStk:        12 kB
VmExe:       300 kB
VmLib:      2528 kB
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000001000
SigCgt: 0000000000014005
CapInh: 0000000000000000
CapPrm: 00000000ffffeff
CapEff: 00000000ffffeff
```

Más que el nombre y el ID del proceso, tiene a su disposción el estado (por ejemplo `S (sleeping)` o `R (running)`) y el ID de usuario/grupo al ejecutar el proceso, así como datos muy detallados sobre el uso de la memoria.

2.3.1.1. `/proc/self`

El directorio `/proc/self` es un enlace al proceso en ejecución. Esto le permite verse a si mismo sin tener que conocer su ID de proceso.

Dentro de un entorno de la shell, una lista del directorio `/proc/self` produce el mismo contendido que una lista del directorio del proceso para ese proceso.

2.3.2. `/proc/bus/`

Este directorio contiene información específica sobre los diversos busses disponibles en el sistema. Por ejemplo, en un sistema estándar que contenga busses ISA, PCI y USB, los datos actuales de cada uno de estos busses están disponibles en el directorio bajo `/proc/bus/`.

Los contenidos de los subdirectorios y ficheros disponibles varían según la configuración precisa de su sistema. No obstante, cada uno de los directorios para cada uno de los tipos de bus contiene al menos un directorio para cada bus de ese tipo. Estos directorios bus individuales, habitualmente comunidados con números, tales como `00` contienen ficheros binarios que se refieren a los varios dispositivos disponibles en ese bus.

Por ejemplo, un sistema con un bus USB sin ningún USB conectado a este tiene un directorio `/proc/bus/usb` que contiene varios ficheros:

```
total 0
dr-xr-xr-x    1 root     root            0 May  3 16:25 001
-r--r--r--    1 root     root            0 May  3 16:25 devices
-r--r--r--    1 root     root            0 May  3 16:25 drivers
```

El directorio `/proc/bus/usb` contiene ficheros que siguen los diferentes dispositivos en cualquier bus USB, así como los controladores requeridos para su uso. El directorio `001` contiene todos los dispositivos del primer (y único) bus USB. Al mirar el contenido del fichero `devices` podemos ver que se trata del hub raíz de USB de la placa madre.

```
T:  Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#=  1 Spd=12  MxCh= 2
B:  Alloc=  0/900 us ( 0%), #Int=  0, #Iso=  0
D:  Ver= 1.00 Cls=09(hub  ) Sub=00 Prot=00 MxPS= 8 #Cfgs=  1
P:  Vendor=0000 ProdID=0000 Rev= 0.00
```

```
S:  Product=USB UHCI Root Hub
S:  SerialNumber=d400
C:* #Ifs= 1 Cfg#= 1 Atr=40 MxPwr=  0mA
I:  If#= 0 Alt= 0 #EPs= 1 Cls=09(hub  ) Sub=00 Prot=00 Driver=hub
E:  Ad=81(I) Atr=03(Int.) MxPS=   8 Ivl=255ms
```

2.3.3. /proc/driver/

Este directorio contiene información para drivers específicos que el kernel está utilizando.

`rtc` es un fichero habitual aquíe que proporciona salida desde el driver para el *Real Time Clock (RTC)* del sistema, dispositivo que guarda el tiempo mientras que el sistema está apagado. Un ejemplo de salida de datos desde `/proc/driver/rtc`:

```
rtc_time : 01:38:43
rtc_date : 1998-02-13
rtc_epoch : 1900
alarm  : 00:00:00
DST_enable : no
BCD  : yes
24hr  : yes
square_wave : no
alarm_IRQ : no
update_IRQ : no
periodic_IRQ : no
periodic_freq : 1024
batt_status : okay
```

Para obtener más información sobre el RTC, revise `/usr/src/linux-2.4/Documentation/rtc.txt`.

2.3.4. /proc/ide/

Este directorio contiene una cantidad muy surtida de información sobre los dispositivos IDE del sistema. Cada canal IDE está representado como un directorio separado, como `/proc/ide/ide0` y `/proc/ide/ide1`. Además, un fichero `drivers` también está disponible, al proporcionar el número de versión de varios drivers usados en los canales IDE:

```
ide-cdrom version 4.59
ide-floppy version 0.97
ide-disk version 1.10
```

Muchos chipsets proporcionan un fichero de información en este directorio que aporta datos adicionales referentes a las unidades conectadas a través de varios canales. Por ejemplo, un chipset genérico Intel PIIX4 Ultra 33 produce un `/proc/ide/piix` que le informará de si DMA o UDMA está o no habilitado para los dispositivos en los canales IDE:

```
                                Intel PIIX4 Ultra 33 Chipset.
------------- Primary Channel ---------------- Secondary Channel -------------

                 enabled                           enabled
------------- drive0 --------- drive1 -------- drive0 ---------- drive1 ------
```

```
DMA enabled:    yes             no              yes             no
UDMA enabled:   yes             no              no              no
UDMA enabled:   2               X               X               X
UDMA
DMA
PIO
```

Al navegar en un directorio para un canal IDE, como `ide0` para el primer canal, obtendrá más información. El fichero `channel` proporciona el número de canal, mientras que `model` le facilita el tipo de bus para el canal (como `pci`).

2.3.4.1. Directorios de dispositivo

Cada directorio del canal IDE es un directorio del dispositivo. El nombre del directorio del dispositivo corresponde a la letra del dispositivo en el directorio `/dev`. Por ejemplo el primer dispositivo IDE drive en `ide0` es `hda`.

Nota

Existe un symlink para cada uno de estos directorios de dispositivos en el directorio `/proc/ide/`.

Cada dispositivo, como un disco duro o un CD-ROM, tendrá en ese canal su propio directorio en el que están incluidas su propia recopilación de información y estadísticas. Los contenidos de esos directorios varían de acuerdo con el tipo de dispositivo conectado. Algunos de los ficheros más útiles habituales en diferentes dispositivos incluyen:

- `cache` — La caché del dispositivo.
- `capacity` — La capacidad del dispositivo, en bloques de 512 bytes.
- `driver` — El driver y la versión usados para controlar el dispositivo.
- `geometry` — La geometría física y lógica del dispositivo.
- `media` — El tipo de dispositivo, como por ejemplo un `disk`.
- `model` — El nombre del modelo del dispositivo.
- `settings` — Recopilación de parámetros actuales del dispositivo. Este fichero habitualmente contiene bastante información técnica útil. Un ejemplo de fichero `settings` para un disco duro IDE estándar:

```
name                value           min           max           mode
----                -----           ---           ---           ----
bios_cyl            784             0             65535         rw
bios_head           255             0             255           rw
bios_sect           63              0             63            rw
breada_readahead    4               0             127           rw
bswap               0               0             1             r
current_speed       66              0             69            rw
file_readahead      0               0             2097151       rw
ide_scsi            0               0             1             rw
init_speed          66              0             69            rw
io_32bit            0               0             3             rw
keepsettings        0               0             1             rw
lun                 0               0             7             rw
max_kb_per_request  64              1             127           rw
multcount           8               0             8             rw
nice1               1               0             1             rw
```

```
nowerr              0             0           1           rw
number              0             0           3           rw
pio_mode            write-only    0           255         w
slow                0             0           1           rw
unmaskirq           0             0           1           rw
using_dma           1             0           1           rw
```

2.3.5. /proc/irq/

Este directorio se usa para configurar la afinidad de una IRQ con una CPU, lo que le permite conectar una IRQ particular a una sola CPU. De manera alternativa, puede evitar que una CPU manipule cualquier IRQ.

Cada IRQ tiene su propio directorio, permitiendo que cada IRQ sea configurada de forma diferente al otro. El fichero `/proc/irq/prof_cpu_mask` es una máscara de bits que contiene los valores predeterminados para el fichero `smp_affinity` en el directorio de IRQ. Los valores en `smp_affinity` especifican qué CPUs manipulan esa IRQ en particular.

Tiene a su disposición más información en `/usr/src/linux-2.4/Documentation/filesystems/proc.txt`

2.3.6. /proc/net/

El directorio proporciona una visión exhaustiva de diversos parámetros y estadísticas de red. Cada uno de los ficheros cubre una cantidad específica de información relacionada con la red en el sistema:

- `arp` — Contiene la tabla del kernel ARP. Este fichero es particularmente útil para conectar la dirección del hardware a una dirección IP de un sistema.
- `atm` — Directorio que contiene ficheros con diversas configuraciones y estadísticas *Asynchronous Transfer Mode (ATM)* y las tarjetas ASDL.
- `dev` — Lista los diferentes dispositivos de red configurados en en sistema, completa con transmisión y recibe estadísticas. Este fichero le indica el número de paquetes de entrada y de salida, el número de errores, el número de paquetes eliminados, etc.
- `dev_mcast` — Visualiza los diversos grupos Layer2 con destinatario múltiple a los que cada dispositivo escucha.
- `igmp` — Lista las direcciones IP con destinatarios múltiples a las que el sistema se ha incorporado.
- `ip_fwchains` — Revela cualquier cadena del firewall actual.
- `ip_fwnames` — Lista todos los nombres de cadenas del firewall.
- `ip_masquerade` — Proporciona una tabla de información de masquerading.
- `ip_mr_cache` — Lista de la caché de routing de múltiple destinatario.
- `ip_mr_vif` — Lista de las interfaces virtuales de múltiple destinatario.
- `netstat` — Contiene una amplia colección de estadísticas de red, incluyendo la temporización TCP, los cookies enviados y recibidos y mucho más.
- `psched` — Lista de parámetros de planificación global del paquete.
- `raw` — Lista de estadísticas de dispositivo raw.
- `route` — Visualiza la tabla de ruta del kernel.
- `rt_cache` — Contiene la caché de ruta actual.

- snmp — Lista de los datos del protocolo Simple Network Management Protocol (SNMP) para varios protocolos de red en uso.
- sockstat — Proporciona estadísticas de socket.
- tcp — Contiene información detallada del socket TCP.
- tr_rif — Tabla de routing RIF del token ring.
- udp — Contiene información detallada del socket UDP.
- unix — Lista sockets de dominio UNIX.
- wireless — Lista datos de la interfaz de radio.

2.3.7. /proc/scsi/

Del mismo modo el directorio /proc/ide solo existe si un controlador IDE está conectado al sistema, el directorio /proc/scsi sólo está disponible si tiene un adaptador de host SCSI.

El fichero primario aquí es /proc/scsi/scsi, que contiene una lista de cada dispositivo SCSI reorganizado. Por ejemplo, si un sistema contiene un CD-ROM SCSI, unidad de cassette, discos duros y un controlador RAID, el fichero se parecerá a:

```
Attached devices:
Host: scsi1 Channel: 00 Id: 05 Lun: 00
  Vendor: NEC      Model: CD-ROM DRIVE:466 Rev: 1.06
  Type:   CD-ROM                           ANSI SCSI revision: 02
Host: scsi1 Channel: 00 Id: 06 Lun: 00
  Vendor: ARCHIVE  Model: Python 04106-XXX Rev: 7350
  Type:   Sequential-Access                ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 06 Lun: 00
  Vendor: DELL     Model: 1x6 U2W SCSI BP  Rev: 5.35
  Type:   Processor                        ANSI SCSI revision: 02
Host: scsi2 Channel: 02 Id: 00 Lun: 00
  Vendor: MegaRAID Model: LD0 RAID5 34556R Rev: 1.01
  Type:   Direct-Access                    ANSI SCSI revision: 02
```

Además, cada driver SCSI usado por el sistema tiene su propio directorio en /proc/scsi que contiene ficheros específicos para cada controlador SCSI que utiliza aquel driver. En el ejemplo anterior de sistema, los directorios aic7xxx y megaraid están presentes, como aquellos dos drivers que se están utilizando. Los ficheros en cada uno de los directorios contienen típicamenteextensión de dirección de entrada y de salida, IRQ y estadísticas par el controlador especial SCSI que utiliza aquel driver. Mientras que cada controlador remite un tipo y cantidad de información diferente, la salida de datos de la mayoría de estos ficheros resultará de fácil lectura y gran ayuda. El fichero de adaptador de host SCSI Adaptec AIC-7880 Ultra del ejemplo se vería de la siguiente manera:

```
Adaptec AIC7xxx driver version: 5.1.20/3.2.4
Compile Options:
  TCQ Enabled By Default : Disabled
  AIC7XXX_PROC_STATS     : Enabled
  AIC7XXX_RESET_DELAY    : 5

Adapter Configuration:
           SCSI Adapter: Adaptec AIC-7880 Ultra SCSI host adapter
                         Ultra Narrow Controller
    PCI MMAPed I/O Base: 0xfcffe000
 Adapter SEEPROM Config: SEEPROM found and used.
      Adaptec SCSI BIOS: Enabled
                    IRQ: 30
```

```
                  SCBs: Active 0, Max Active 1,
                        Allocated 15, HW 16, Page 255
            Interrupts: 33726
      BIOS Control Word: 0x18a6
   Adapter Control Word: 0x1c5f
   Extended Translation: Enabled
Disconnect Enable Flags: 0x00ff
     Ultra Enable Flags: 0x0020
 Tag Queue Enable Flags: 0x0000
Ordered Queue Tag Flags: 0x0000
Default Tag Queue Depth: 8
    Tagged Queue By Device array for aic7xxx host instance 1:
      {255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255}
    Actual queue depth per device for aic7xxx host instance 1:
      {1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1}

Statistics:


(scsi1:0:5:0)
  Device using Narrow/Sync transfers at 20.0 MByte/sec, offset 15
  Transinfo settings: current(12/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 0 (0 reads and 0 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0       0       0       0       0       0       0       0
  Writes:       0       0       0       0       0       0       0       0


(scsi1:0:6:0)
  Device using Narrow/Sync transfers at 10.0 MByte/sec, offset 15
  Transinfo settings: current(25/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 132 (0 reads and 132 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0       0       0       0       0       0       0       0
  Writes:       0       0       0       1     131       0       0       0
```

En esta pantalla, se puede ver la velocidad de transmisión a los diversos dispositivos SCSI conectados al controlador basado en el canal ID, así como estadísticas detalladas referentes a la cantidad y tamaño de los ficheros leídos o escritos por ese dispositivo. En referencia al fichero `/proc/scsi/scsi`, se puede ver que este controlador está comunicándose con el CD-ROM a 20 megabits por segundo, mientras que la unidad de cassette tan sólo está conectada a 10 megabits por segundo.

2.3.8. `/proc/sys/`

Este directorio es especial y diferente de los otros directorios en `/proc`, ya que no sólo proporciona mucha información sobre el sistema sino que también le permite hacer cambios en la configuración de un kernel en ejecución.

Aviso

Nunca intente cambiar la configuración de su kernel en un sistema de producción usando los diversos ficheros del directorio `/proc/sys`. En ocasiones, el cambio de la configuración puede ocasionar que el kernel no sea estable y que sea necesario rearrancar el sistema.

Antes de intentar cambiar un valor en `/proc/sys`, asegúrese de que conoce las opciones válidas para aquel fichero y el resultado esperado.

Una buena forma de determinar si un fichero particular se puede configurar o si tan sólo está diseñado para proporcionar información y listarla. Si se puede escribir en el fichero, podrá utilizarlo para configurar el kernel de algún modo. Por ejemplo, un listado parcial de `/proc/sys/fs` sería de la siguiente manera:

```
-r--r--r--    1 root     root            0 May 10 16:14 dentry-state
-rw-r--r--    1 root     root            0 May 10 16:14 dir-notify-enable
-r--r--r--    1 root     root            0 May 10 16:14 dquot-nr
-rw-r--r--    1 root     root            0 May 10 16:14 file-max
-r--r--r--    1 root     root            0 May 10 16:14 file-nr
```

En este listado, los ficheros `dir-notify-enable` y `file-max` pueden escribirse y, por consiguiente, usarse para la configuración del kernel. Los otros ficheros sólo provocan reacción en la configuración actual del kernel.

Para cambiar un valor en el fichero `/proc/sys` tiene que repetir el valor nuevo en el fichero. Por ejemplo, para habilitar la System Request Key en un kernel en ejecución, escriba el comando:

```
echo 1 > /proc/sys/kernel/sysrq
```

Esto cambiará el valor del fichero `sysrq` desde `0` a `1`.

El objetivo de la System Request Key es el de permitirle que usted mismo instruya al kernel para realizar un número de actividades importantes mediante el uso de una combinación de claves sencilla, como apagar y reiniciar el sistema inmediatamente, sincronizar todos los sistemas de ficheros o descargar información importante en su consola. Esta característica es más útil cuando se utiliza un kernel de desarrollo o si está experimentando bloqueos del sistema. Para obtener más información sobre la clave de petición de sistema, remítase a `/usr/src/linux-2.4/Documentation/sysrq.txt`.

Unos cuantos ficheros de configuración `/proc/sys` contienen más de un valor. Para enviar valores correctamente, coloque espacio entre cada valor traspasado con el comando `echo`, como se ha hecho a continuación.

```
echo 4 2 45 > /proc/sys/kernel/acct
```

Nota

Cualquier cambio de configuración que haga mediante el comando `echo` repitiendo valores en los ficheros `/proc/sys` desaparecerá cuando vuelva a iniciarse el sistema. Para hacer cambios de configuración llévelos a cabo en el momento en que el sistema arranque, vea la Sección 2.4.

El directorio`/proc/sys` contiene directorios diferentes que controlan diferentes aspectos de la ejecución de un kernel.

2.3.8.1. /proc/sys/dev/

Este directorio proporciona parámetros para dispositivos particulares en el sistema. La mayoría de sistemas tienen al menos dos directorios `cdrom` y `raid`, sin embargo, los kernels personalizados pueden tener otros, como por ejemplo `parport`, que proporciona la habilidad de compartir un puerto paralelo entre drivers de dispositivo múltiple.

El directorio `cdrom` contiene un fichero llamado `info`, que revela algunos parámetros importantes de CD-ROM:

```
CD-ROM information, Id: cdrom.c 3.12 2000/10/18

drive name:  hdc
drive speed:  32
drive # of slots: 1
Can close tray:  1
Can open tray:  1
Can lock tray:  1
Can change speed: 1
Can select disk: 0
Can read multisession: 1
Can read MCN:  1
Reports media changed: 1
Can play audio:  1
Can write CD-R:  0
Can write CD-RW: 0
Can read DVD:  0
Can write DVD-R: 0
Can write DVD-RAM: 0
```

Este fichero se puede escanear con la finalidad de descubrir las cualidades de un CD-ROM desconocido, por lo menos para el kernel. Si tiene a su disposición múltiples CD-ROMs en un sistema, cada dispositivo tendrá su propia columna de información.

Se pueden utilizar diversos ficheros en `/proc/sys/dev/cdrom`, como `autoclose` y `checkmedia`, para controlar el CD-ROM del sistema. Sencillamente `echo` un `1` para el correcto fichero y de este modo habilitar la característica o un `0` para deshabilitarla.

Si se se compila el soporte RAID en el kernel, tendrá a su disposición un directorio `/proc/sys/dev/raid` con, al menos, dos ficheros dentro del mismo: `speed_limit_min` y `speed_limit_max`. Estas configuraciones se dan para aminorar o acelerar la velocidad en que se utiliza el dispositivo RAID para tareas intensivas de entrada y salida en particular, tales como la resincronización de los discos.

2.3.8.2. /proc/sys/fs/

Este directorio contiene un compendio de opciones y de información referente a varios aspectos del sistema de ficheros, incluyendo la información quota, manipulación del fichero, inode y dentry.

El directorio `binfmt_misc` se usa para proporcionar soporte del kernel para varios formatos binarios.

Los ficheros importantes en `/proc/sys/fs` incluyen:

- `dentry-state` — Proporciona el estado de la caché del directorio. El fichero se vería de la siguiente manera:

  ```
  57411 52939 45 0 0 0
  ```

  El primer número revela el número total de las entradas de la caché del directorio, mientras que el segundo número visualiza el número de entradas inutilizadas. El tercero, le indica el número de

segundos en que un directorio ha sido liberado y puede ser reclamado y el cuarto mide las páginas que han sido requeridas por el sistema en la actualidad. Los últimos dos números no están e uso y tan sólo visualizan ceros.

- `dquot-nr` — Muestra el número máximo de entradas de quota de disco cacheado.
- `file-max` — Permite cambiar el número máximo de manipulación de ficheros que asignará el kernel. Si alza el valor de este fichero resolverá los errores causados por la falta de manipulación de ficheros disponibles.
- `file-nr` — Visualiza el número de manipulación de ficheros asignados, manipulación de ficheros usados, así como el número máximo de manipulación de ficheros, en este orden.
- `overflowgid` y `overflowuid` — Define el ID de grupo establecido y el ID de usuario, respectivamente, para el uso con el sistema de ficheros que tan sólo soporta los IDs de grupo y usuario de 16 bits.
- `super-max` — Controla el número máximo de superbloques disponible.
- `super-nr` — Visualiza el número actual de superbloques en uso.

2.3.8.3. `/proc/sys/kernel/`

Este directorio contiene una variedad de ficheros de configuración diferentes que afectan directamente a la operación del kernel. Algunos de los ficheros más importantes incluyen:

- `acct` — Controla la suspensión del proceso de contabilización basado en el porcentaje de espacio libre disponible en el sistema de ficheros que contienen el log. El fichero aparecerá de la siguiente manera, por defecto:

  ```
  4 2 30
  ```

  El segundo valor fija el porcentaje mínimo de espacio libre cuando el registro quede en suspensión, mientras que el primer valor dicta el porcentaje de espacio libre requerido por el registro para continuar. El tercer valor fija el intervalo en segundos en que el kernel interroga al sistema de ficheros para ver si el registro se suspende o continua.
- `cap-bound` — Controla las configuraciones de las opciones de *capacidad de bounding* que proporcionan una lista de capacidades que cualquier proceso del sistema puede realizar. Si una capacidad no está listada aquí, ningún proceso, por muy privilegiado que sea éste, puede realizarlo. La idea inicial es hacer que el sistema sea más seguro asegurando que no acontezcan ciertas cosas, por lo menos llegados a un cierto nivel del proceso de arranque.

  Los posibles diversos valores se escapan del alcance de este manual, consulte la documentación del kernel para más información.
- `ctrl-alt-del` — Controla que [Ctrl]-[Alt]-[Delete] reinicien el ordenador mediante el uso de `init` (valor `0`) o fuercen un rearranque inmediato si la sincronización de buffers modificados para el disco (valor `1`).
- `domainname` — Le permite configurar el nombre de dominio del sistema, como `domain.com`.
- `hostname` — Le permite configurar el nombre del host del sistema, como `host.domain.com`.
- `hotplug` — Configura la utilidad para que ésta sea usada cuando se detecta un cambio en la configuración del sistema. Principalmente se usa con USB y Cardbus PCI. El valor por defecto de `/sbin/hotplug` no debería ser cambiado a menos que esté probando un nuevo programa para cumplir con este papel.
- `modprobe` — Fija la ubicación del programa a usar para cargar los módulos del kernel cuando éstos sean necesarios. El valor por defecto de `/sbin/modprobe` significa que `kmod` lo solicitará para cargar el módulo cuando un thread del kernel solicite `kmod`.

- `msgmax` — Fija el tamaño máximo de cualquier mensaje enviado desde un proceso a otro, que está fijado en `8192` bytes por defecto. Debería tener cuidado al alzar este valor, ya que los mensajes en cola entre procesos están almacenados en una memoria de kernel sin memoria de intercambio y cualquier aumento en `msgmax` incrementará los requisitos de RAM para el sistema.
- `msgmnb` — Establece el número máximo de bytes en una única cola de mensajes. Por defecto, `16384`.
- `msgmni` — Establece el número máximo de identificadores de la cola de mensajes. Por defecto, `16`.
- `osrelease` — Lista el número de versión del kernel de Linux. Este fichero tan sólo puede ser alterado al cambiar la fuente del kernel y recompilarla.
- `ostype` — Visualiza el tipo de sistema operativo. Por defecto, este fichero está configurado para `Linux` y este valor tan sólo puede ser cambiado al cambiar la fuente del kernel y recompilarla.
- `overflowgid` y `overflowuid` — Define el ID de grupo establecido y el ID de usuario, respectivamente, para el uso con llamadas del sistema a arquitecturas que tan sólo soportan IDs de grupo y usuario de 16 bits.
- `panic` — Define el número de segundos que el kernel pospone el arranque del sistema cuando se experimenta una emergencia en el kernel. Por defecto, el valor está establecido en `0`, lo que deshabilita el rearranque automático tras una emergencia.
- `printk` — Este fichero controla una variedad de configuraciones relacionadas con la impresión o los mensajes de error de registro. Cada mensaje de error remitido por el kernel tiene un *loglevel* asociado a éste que define la importancia del mensaje. Los valores de loglevel aparecen en el orden siguiente:
  - `0` — Emergencia del Kernel. No se puede utilizar el sistema.
  - `1` — Alerta del kernel. Se debe actuar inmediatamente.
  - `2` — La condición del kernel se considera crítica.
  - `3` — Condición de error general del kernel.
  - `4` — Condición de aviso general del kernel.
  - `5` — Nota del kernel de una condición normal pero significativa.
  - `6` — Mensaje informativo del kernel.
  - `7` — Mensajes de depuración del kernel.

  En el fichero `printk` aparecen cuatro valores:
  ```
  6 4 1 7
  ```
  Cada uno de estos valores define una regla diferente para tratar con los mensajes de error. El primer valor, llamado *console loglevel*, define la prioridad más baja de mensajes que se imprimirán en la consola. (Observe que, cuanto más baja sea ésta, más alto será el número de loglevel.) El segundo valor establece el loglevel por defecto para mensajes adjuntos a éstos sin un loglevel explícito. El tercer valor establece la configuración del loglevel lo más bajo posible para el loglevel de la consola. El último valor establece el valor por defecto para el loglevel de la consola.
- `rtsig-max` — Configura el número máximo de señales en tiempo real POSIX que el sistema podría haber puesto en cola en cualquier otro momento. El valor por defecto es `1024`.
- `rtsig-nr` — El número actual de señales POIX en tiempo real que el kernel ha puesto en cola.
- `sem` — Este fichero establece las configuraciones del semáforo interior del kernel. Un *semáforo* es un objeto System V IPC usado para controlar el uso de un proceso en particular.
- `shmall` — Establece la cantidad total de memoria que se puede utilizar de una sola vez en el sistema, en bytes. Por defecto, este valor es `2097152`.

- shmmax — Establece el mayor tamaño de segmento de memoria compartida que permite el kernel, en bytes. Por defecto, este valor es 33554432. No obstante, el kernel soporta valores con mucho más margen.
- shmmni — Establece el número máximo de segmentos de memoria compartida para todo el sistema. Por defecto, este valor es 4096.
- sysrq — Activa la clave de petición de sistema, si el valor difiere del establecido por defecto 0. Ver la Sección 2.3.8 para mayor información sobre la System Request Key.
- threads-max — Establece el número máximo de threads que puede usar el kernel, con un valor por defecto de 2048.
- version — Visualiza la fecha y la hora en los que el kernel fue completado por última vez. El primer campo en este fichero, #3, está relacionado con el número de veces que se ha construido un kernel desde la base de la fuente.

El directorio random almacena un número de valores relacionados a la generación de números aleatorios para el kernel.

2.3.8.4. /proc/sys/net

Este directorio contiene diversos directorios que tratan tópicos acerca de red, incluyendo protocolos variados y centros de énfasis. La disponibilidad de diferentes directorios es posible gracias a algunas configuraciones realizadas durante la compilación del kernel, tales como appletalk, ethernet, ipv4, ipx y ipv6. Dentro de estos directorios, podrá ajustar los diversos valores de red para esa configuración en un sistema en funcionamiento.

Debido a la amplia variedad de posibles opciones de red disponibles con Linux y la gran cantidad de espacio requerido para comentarlas, tan sólo se comentarán los directorios /proc/sys/net más habituales.

El directorio core contiene una variedad de configuraciones que controlan la interacción entre el kernel y las capas de red. Los ficheros más importantes son:

- message_burst — Décimas de segundos requeridos para escribir un mensaje nuevo de aviso. Se usa para prevenir ataques Denial of Service (DoS) y la configuración por defecto es 50.
- message_cost — También se utiliza para prevenir ataques de DoS poniendo un coste a cada mensaje de aviso. Cuanto más alto es el valor de este fichero (por defecto 5), más probable es que el aviso del mensaje sea ignorado.

  La idea es que un agresor podría bombardear su sistema con peticiones que generen errores y llenen sus logs o necesiten todos los recursos del sistema para manipular el registro de errores. Las configuraciones en message_burst y message_cost están diseñadas para ser modificadas basándose el riesgo aceptable del sistema contra la necesidad de un registro exhaustivo.
- netdev_max_backlog — Establece el número máximo de paquetes permitido para hacer cola cuando una interfaz en particular recibe paquetes a una velocidad superior a la que el kernel puede procesarlos. El valor por defecto para este fichero es 300.
- optmem_max — Configura el tamaño máximo de buffer secundario por socket.
- rmem_default — Establece el tamaño por defecto del buffer del socket de recepción en bytes.
- rmem_max — Establece el tamaño máximo del buffer de recepción en bytes.
- wmem_default — Establece el tamaño por defecto del buffer del socket de enviar en bytes.
- wmem_max — Establece el tamaño máximo de la buffer del socket de enviar en bytes.

Teniendo en cuenta lo extendido que está el uso de las redes IP con Linux, la consulta de los ficheros más importantes en ipv4 revela configuraciones de red de gran potencia. Muchas de estas config-

uraciones, usadas conjuntamente con otras, resultan muy útiles para la prevención de ataques en su sistema.

Aviso

No obstante, asegúrese de que sabe lo que está haciendo, tan bien como lo que espera que suceda, antes de cambiar cualquiera de estas configuraciones. Otra cosa a tener en cuenta es que los cambios los ha de hacer localmente, ya que un cambio erróneo podría afectar a la conectividad remota de su sistema.

Aquí tiene algunos de los ficheros más importantes en el directorio `ipv4`:

- `icmp_destunreach_rate`, `icmp_echoreply_rate`, `icmp_paramprob_rate` y `icmp_timeexeed_rate` — Establece el ratio máximo de paquetes ICMP a enviar, en centésimas de un segundo en sistemas Intel, para hosts bajo diversas condiciones. Una configuración de `0` elimina cualquier retraso y no es una buena idea.
- `icmp_echo_ignore_all` and `icmp_echo_ignore_broadcasts` — Permite que el kernel ignore paquetes ICMP ECHO desde cada host o tan sólo aquéllos que se originen desde direcciones broadcast y de destinatario múltiple, respectivamente. `0` permite que el kernel responda, mientras un `1` ignora los paquetes.
- `ip_default_ttl` — Establece el *Time To Live (TTL)* predeterminado, que limita el número de saltos que un paquete puede efectuar antes de alcanzar su destino. Si incrementa este valor, la ejecución del sistema puede disminuir.
- `ip_forward` — Permite interfaces en el sistema para reenviar paquetes a otro. Por defecto, este fichero está fijado en `0` para deshabilitar el reenvío; sin embargo, si fija este fichero en `1` habilitará el reenvío.
- `ip_local_port_range` — Especifica la extensión de puertos a usar por TCP o UDP cuando es necesario un puerto local. El primer número es el puerto más bajo que puede utilizar, y el segundo especifica el puerto más alto. Cualquier sistema que se crea que necesitará más puertos que los predeterminados 1024 hasta 4999 debería usar la extensión 32768 hasta 61000S en este fichero.
- `tcp_syn_retries` — Proporciona un límite en el número de veces que se intenta acceder a una conexión.
- `tcp_retries1` — Establece el número de retransmisiones permitidas que intentan responder una conexión de entrada. `3` por defecto.
- `tcp_retries2` — Establece el número de retransmisiones permitidas de paquetes TCP. `15` por defecto.

Para consultar la lista completa de ficheros y opciones, vea `/usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt`.

Existe un número de otros directorios dentro del directorio `/proc/sys/net/ipv4` que cubren temas más específicos. El directorio `conf` permite que cada una de las interfaces del sistema sea configurada de diferentes formas,incluyendo el uso de configuraciones por defecto para dispositivos sin configurar (en el subdirectorio `default`) y configuraciones que sobreescriben todas las configuraciones especiales (en el subdirectorio `all`).

Para controlar las conexiones entre "vecinos" directos, es decir, cualquier otro sistema directamente conectado a su sistema, el directorio `neigh` acepta configuraciones especiales para cada interfaz. Del mismo modo, también facilita la implantación de reglas estrictas para sistemas que están distanciados por varios saltos. away.

Routing por encima de IPV4 también tiene su propio directorio, `route`. A diferencia de `conf` y `neigh`, el directorio `route` contiene especificaciones que se aplican a routing con cualquier in-

terfaz del sistema. Muchas de estas configuraciones, como por ejemplo max_size, max_delay y min_delay están relacionadas con el control del tamaño de la caché de routing. Para borrar la caché de routing, simplemente escriba cualquier valor en el fichero flush.

Encontrará información adicional sobre estos directorios y los posibles valores de sus ficheros de configuración en /usr/src/linux-2.4/Documentation/filesystems/proc.txt.

2.3.8.5. /proc/sys/vm/

Este directorio facilita la configuración del subsistema de memoria virtual (VM) del kernel. El kernel hace un uso extensivo e inteligente de la memoria virtual, conocida comunmente como espacio swap.

Los siguientes ficheros se encuentran habitualmente en el directorio /proc/sys/vm:

- bdflush — Establece varios valores relacionados con el demonio del kernel bdflush.
- buffermem — Le permite controlar la cantidad porcentual de la memoria total del sistema a usar para la memoria del buffer. Salida de datos típica para este fichero:
  ```
  2       10       60
  ```
  Los primeros y últimos valores establecen el porcentaje mínimo y máximo de memoria que ha de usarse como memoria de buffer, respectivamente. El valor del medio establece el porcentaje de memoria del sistema dedicado a la memoria de buffer donde el subsistema de gestión de memoria iniciará borrando la caché del buffer más que otros tipos de memoria para compensar la falta en general de memoria libre.
- freepages — Visualiza varios valores relacionados con páginas libres de memoria del sistema. Ejemplo:
  ```
  512 768 1024
  ```
  El primer valor muestra el número mínimo de páginas libres permitido antes de que el kernel asuma el control de la asignación de la memoria adicional. El segundo valor da el número de páginas libres antes de que el kernel empiece hacer swap para preservar la ejecución. El tercer valor es el número de páginas libres que el sistema mantiene siempre disponibles.
- kswapd — Establece varios valores referentes al demonio de swap-out del kernel, kswapd. Este fichero tiene tres valores:
  ```
  512 32 8
  ```
  El primer valor establece el número máximo de páginas que kswapd intentará liberar en una sola vez. Cuanto mayor sea el número, más enérgico será el kernel al liberar páginas. El segundo valor establece el número mínimo de veces que kswapd intenta dejar libre una página. El tercer valor establece el número de páginas kswapd escribir en un solo intento. Una correcta sintonización de este valor final puede mejorar la ejecución de un sistema usando mucho espacio swap al hacer que el kernel escriba páginas en grandes cantidades, minimizando el número de búsquedas de disco.
- max_map_count — Configura el número máximo de áreas de mapa de memoria que puede tener un proceso. En la mayoría de los casos, el valor por defecto de 65536 es apropiado.
- overcommit_memory — Contiene un valor, que cuando no es el predeterminado 0, permite al kernel saltarse un chequeo estándar para ver si existe suficiente memoria antes de asignarlo.

  Si el valor de overcommit_memory es1, se aumenta la sobrecarga del sistema pero haya que decir que la memoria que se usa para este tipo de tareas intensas equivale a la que usan los softwarea científicos.

  Para los usuarios que no quieren correr risgos en la memoria, existen dos opciones. El valor de overcommit_memory 2 falla si se añade más de la mitad de la memoria RAM y una partición swap. En 3 falla si se requiere una memoria mayor de la que uns partición swap puede mantener.

- pagecache — Controla la cantidad de memoria usada por la caché de la página. Los valores en pagecache son porcentajes y funcionan de manera parecida a buffermem para reforzar los mínimos y los máximos de memoria caché de página disponible.
- page-cluster — Establece el número de páginas leídas en un solo intento. El valor por defecto de 4 establecido en 16 páginas, es apropiado para la mayoría de los sistemas.
- pagetable_cache — Controla el número de tablas de página que están cacheadas en las bases para un procesador. Los primeros y segundos valores están relacionados con el número mínimo y máximo de tablas de página a establecer aparte, respectivamente.

Encontrará información adicional sobre estos ficheros en /usr/src/linux-2.4/Documentation/sysctl/vm.txt.

2.3.9. /proc/sysvipc

Este directorio contiene información sobre los recursos System V IPC. Los ficheros de este directorio están relacionados con las llamadas al System V IPC para mensajes (msg), semáforos (sem) y memoria compartida (shm).

2.3.10. /proc/tty/

Este directorio contiene información sobre los dispositivos tty del sistema. Conocido originariamente como un *dispositivo teletype*, a cualquier terminal de datos basado en caracteres se le conoce como *dispositivox tty*.

En Linux existen tres tipos diferentes de dispositivos tty. Los *dispositivos de serie* se usan con conexiones de serie, tales como un módem o el uso de un cable de serie. Los *Terminales virtuales* crean las conexiones de consola comunes, tales como las consolas virtuales disponibles al pulsar [Alt]-[<F-key>] en la consola del sistema. Los *terminales pseudo* crean una comunicación de dos sentidos que usan las aplicaciones de nivel alto, tales como **X11**.

El fichero drivers es una lista de dispositivos tty actualmente en uso:

```
serial               /dev/cua        5  64-127 serial:callout
serial               /dev/ttyS       4  64-127 serial
pty_slave            /dev/pts      136   0-255 pty:slave
pty_master           /dev/ptm      128   0-255 pty:master
pty_slave            /dev/ttyp       3   0-255 pty:slave
pty_master           /dev/pty        2   0-255 pty:master
/dev/vc/0            /dev/vc/0       4       0 system:vtmaster
/dev/ptmx            /dev/ptmx       5       2 system
/dev/console         /dev/console    5       1 system:console
/dev/tty             /dev/tty        5       0 system:/dev/tty
unknown              /dev/vc/%d      4    1-63 console
```

El fichero /proc/tty/driver/serial lista las estadísticas en uso y el estado de cada una de las líneas de serie tty.

Para que se puedan utilizar los dispositivos tty de un modo similar a los dispositivos de red, el kernel de Linux reforzará la *disciplina de línea* en el dispositivo. Esto permite que el controlador coloque un tipo específico de encabezamiento a cada bloque de datos transmitido por el dispositivo, haciendo posible que el final remoto de la conexión vea el bloque de datos como uno más en la línea de bloques de datos. SLIP y PPP son disciplinas de línea comunes y se usan comunmente para conectar sistemas en un enlace serial.

En el fichero ldiscs encontrará disciplinas de líneas registradas, con información detallada en el directorio ldisc.

2.4. Usar sysctl

El establecimiento de los parámetros del kernel en el directorio /proc/sys no tiene que ser un proceso manual o quer requiera la repetición de valores en un fichero virtual, con la esperanza de que éstos sean correctos. El comando sysctl puede visualizar, establecer y automatizar la configuración de un kernel especial fácimente.

Para tener una vista preliminar de todas las configuraciones en el directorio /proc/sys, teclee el comando sysctl -a como root. Esto creará una lista exhaustiva, a continuación le mostramos un pequeño ejemplo:

```
net.ipv4.route.min_delay = 2
kernel.sysrq = 0
kernel.sem = 250     32000     32     128
```

Ésta es la misma información básica que vería si echara un vistazo a cada uno de los ficheros individualmente. La única diferencia es la localización del fichero. /proc/sys/net/ipv4/route/min_delay está representado por net.ipv4.route.min_delay con barras oblicuas del directorio sustituidas por puntos y la porción asumida proc.sys.

El comando sysctl se puede usar en vez de echo para asignar valores a los ficheros en los que se puede escribir en el directorio /proc/sys/ . Por ejemplo, en vez de usar este comando:

```
echo 1 > /proc/sys/kernel/sysrq
```

Puede usar el comando sysctl:

```
sysctl -w kernel.sysrq="1"
kernel.sysrq = 1
```

Establecer rápidamente valores únicos en /proc/sys es útil durante la prueba, no obstante, esto no funciona tan bien en un sistema de producción, ya que todas las configuraciones especiales /proc/sys se pierden cuando se vuelve a arrancar el sistema. Para conservar las configuraciones que quiere establecer como permanentes en su kernel, añádalas al fichero /etc/sysctl.conf.

Cada vez que el sistema arranque, init ejecuta el script /etc/rc.d/rc.sysinit. Este script contiene un comando para ejecutar sysctl mediante el uso de /etc/sysctl.conf como los valores a establecer. Por eso, cualquier valor añadido a /etc/sysctl.conf surtirá efecto una vez que el sistema arranque sin la necesidad de reconfigurar y reconstruir el kernel para incorporar los cambios.

2.5. Recursos adicionales

2.5.1. Documentación instalada

La mayoría de la mejor documentación sobre /proc está disponible en su sistema.

- /usr/src/linux-2.4/Documentation/filesystems/proc.txt — Contiene información variada pero limitada sobre todos los aspectos de /proc.
- /usr/src/linux-2.4/Documentation/sysrq.txt — Vista preliminar de las opciones de System Request Key.

- /usr/src/linux-2.4/Documentation/sysctl — Directorio que contiene una variedad de avisos sysctl, incluyendo valores modificados que hacen referencia al kernel (kernel.txt), accediendo al sistema de ficheros (fs.txt) y el uso de memoria virtual (vm.txt).
- /usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt — Descripción de varias opciones IP de red y lo que significan para el kernel.
- La información más autorizada la encontrará leyendo el código fuente del kernel /proc. Asegúrese de que el RPM de kernel-source está instalado en su sistema y consulte el directorio /usr/src/linux-2.4.

2.5.2. Sitios web útiles

- http://www.linuxhq.com — Este sitio contiene una fuente de base de datos completa, parches y documentación para varias versiones del kernel de Linux.

Capítulo 3.

Proceso de arranque, inicio y cierre del sistema

Una de las características más importantes de Red Hat Linux es el método abierto para el inicio y cierre del sistema operativo. Durante el tiempo de arranque Red Hat Linux carga programas en un orden específico y configurable. Una vez que haya arrancado, podrá cambiar los ficheros de configuración que controlan el proceso de de arranque así como los ficheros de configuración para los programas iniciados en el tiempo de arranque. De forma parecida, el cierre del sistema finaliza los procesos de forma organizada y configurable, aunque la personalización de este proceso no siempre es necesaria.

Entender el funcionamiento del proceso de arranque y cierre no solo le permitirá personalizar fácilmente Red Hat Linux de acuerdo con sus necesidades, sino que también le facilitará resolver problemas relacionados con el incio y el cierre del sistema.

3.1. Proceso de arranque

A continuación obtendrá las etapas básicas del proceso de arranque para un sistema x86:

1. La BIOS del sistema comprueba y lanza la primera etapa del gestor de arranque del MBR del disco duro primario.
2. La primera etapa del gestor de arranque se autocarga en memoria y lanza la seguand etapa del gestor de arranque desde la partición `/boot/`.
3. El kernel se carga en memoria, que a su vez carga cualquier módulo necesario y monta la partición de root en modo sólo lectura.
4. El kernel gestiona el control del proceso de arranque para el programa `/sbin/init`.
5. El programa `/sbin/init` carga todos los servicios y herramientas de espacio del usuario y monta todas las particiones listadas en `/etc/fstab`.
6. El usuario se presenta con un intérprete de comandos de registro para el sistema Linux apenas arrancado.

Ya que la configuración del proceso de arranque es más común que el proceso de personalización y de cierre, lo que queda de capítulo discutirá el modo en el que el proceso de arranque funciona y cómo se puede personalizar para satisfacer sus necesidades.

3.2. Vista detallada del proceso de arranque

El inicio del proceso de arranque varia dependiendo de la plataforma en la que está arrancando Red Hat Linux. Sin embargo, una vez que se encuentra el kernel y se carga el sistema, le proceso de arranque por defecto es idéntico a través de todas las arquitecturas. En el ejemplo mostrado a continuación, el sistema sería un ordenador x86.

3.2.1. La BIOS

Cuando un ordenador x86 computer se carga, el procesador controla el final de la memoria del sistema para *Basic Input/Output System* o el programa *BIOS* y lo ejecuta. La BIOS controla no sólo el primer paso del proceso de arranque,sino que también proporciona una interfaz de bajo nivel para dispositivos periféricos. Por este motivo se escribe tan sólo en modo lectura, memoria permanente y está siempre disponible para el uso.

Otras plataformas usan programas diferentes para ejecutar tareas a bajo nivel equivalentes a aquellas de la BIOS en el sistema x86. Por ejemplo, los ordenadores basados en Itanium usan *Interfaz de Firmware extensible* (*EFI*) *Shell*, mientras que los sistemas Alpha usan *SRM console*.

Una vez que se haya cargado, la BIOS chequea los periféricos y localiza un dispositivo con el que arrancar el sistema. Habitualmente, en primer lugar comprueba cualquier disquete y unidades de CD-ROM presente para los medios de arranque, y a continuación, echa un vistazo a las unidades des de disco duro del sistema. El orden de las unidades necesario para arrancar puede ser controlado con una configuración de la BIOS. A menudo, la primera unidad de disco duro para arrancar es la unidad C o el dispositivo master IDE en el bus primario IDE. La BIOS carga cualquier programa que resida en en el primer sector de este dispositivo, llamado *Master Boot Record* o *MBR* en memoria. El MBR posee tan sólo 512 bytes de tamaño y contiene instrucciones del código de máquina para arrancar la máquina junto a la tabla de particiones. Una vez que haya encontrado y cargado la BIOS pasa el control a cualquier programa del MBR.

3.2.2. El gestor de arranque

Esta sección controla el proceso de arranque para la plataforma x86. Dependiendo de la arquitectura del sistema, el proceso de arranque diferirá ligeramente. Consulte Sección 3.4 para echarle un vistazo a los procesos de arranque de arquitecturas que no sean x86.

Los gestores de arranque de Linux para la plataforma x86 se clasifican en dos etapas. La primera es un código binario de máquina pequeña en el MBR. Su única función es la de localizar el gestor de arranque de la segunda etapa y cargar la primera parte de éste en memoria. Bajo Red Hat Linux podrá instalar un de los dos gestores: *GRUB* o *LILO*. GRUB es el gestor de arranque por defecto, pero LILO está disponible para los usuarios que lo necesiten para su hardware o que sencillamente lo prefieran. Para obtener más información sobre la configuración y el uso de GRUB o LILO, consulte Capítulo 4.

Si está usando LILO bajo Red Hat Linux, la segunda etapa del gestor de arranque es usar la información del MBR para determinar las opciones de arranque disponibles para el usuario. Esto significa que cada vez que se produzca un cambio en la configuración o actualice el kernel de forma manual, debe ejecutar el comando `/sbin/lilo -v -v` para escribir la información para el MBR. Para obtener más detalles sobre como realizarlo, consulte Sección 4.8.

GRUB es capaz de leer particiones ext2 y, por consiguiente, cargar el fichero de configuración — `/boot/grub/grub.conf` — cuando se llama al gestor de la segunda etapa. Consulte Sección 4.7 para obtener información sobre cómo modificar este fichero.

Advertencia

Si actualiza el kernel mediante el uso de **Red Hat Update Agent**, el MBR o the MBR `/boot/grub/grub.conf` serán actualizados automáticamente. Para obtener más información sobre RHN, remítase a la siguiente URL, https://rhn.redhat.com

Una vez que el gestor de arranque de la segunda etapa está en memoria, presenta al usuario con la pantalla inicial, gráfica de Red Hat Linux mostrando los diferentes sistemas operativos o kernels que para los que ha sido configurado para arrancar. Si tan sólo tiene Red Hat Linux instalado y no ha cambiado nada en `/etc/lilo.conf` o `/boot/grub/grub.conf`, verá tan sólo una opción para arrancar.

Si ha configurado el gestor de arranque para arrancar otros sistemas operativos, esta pantalla le dará la oportunidad de seleccionarlo. Utilice las teclas de las fechas para evidenciar el sistema operativo y pulse [Enter]. En caso de no modificar nada, el gestor de arranque cargará la selección por defecto.

Nota

Si ha instalado el soporte para el kernel Symmetric Multi-Processor (SMP), verá más de una opción la primera vez que arranque el sistema. Bajo LILO verá `linux` y `linux-up`. Bajo GRUB verá `Red Hat Linux (`*`kernel version`*`)` y `Red Hat Linux (`*`kernel version-smp`*`)`. La opción `linux` o `Red Hat Linux (`*`kernel version-smp`*`)` es el kernel SMP. Si le surge cualquier problema con el kernel SMP, seleccione `.linux-up` o un kernel que no sea SMP antes antes de rearrancar.

Si necesita cambiar los argumentos de la línea de comandos para el kernel, consulte Capítulo 4. Para obtener más información sobre el cambio del nivel de ejecución en el intérprete de GRUB o LILO, consulte Sección 3.5.

Una vez que el gestor de arranque de la segunda etapa haya determinado qué kernel arrancar, localiza el binario del kernel correspondiente en el directorio `/boot/`. El binario adecuado es el fichero `/boot/vmlinuz-2.4.`*`x-xx`* que corresponde a la configuración del gestor de arranque.Próximo al gestor de arranque se sitúa la imagen adecuada de *initial RAM disk*, conocida como *initrd*, en memoria. El kernel usa `initrd` para cargar cualquier driver sin compilar necesario para arrancar el sistema. Esto es muy importante si posee unidades de disco duro SCSI o si está usando el sistema de ficheros ext3. [1].

Aviso

No elimine el directorio `/initrd/` del sistema de ficheros bajo ningún concepto. Si lo elimina su sistema le dará un mensaje de error de pánico en el tiempo de arranque.

Una vez que el kernel y la imagen *initrd* se cargan en memoria, el gestor de arranque controla el proceso de arranque para el kernel.

3.2.3. El kernel

Cuando el kernel se carga, inmediatamente se inicializa y configura la memoria del ordenador. A continuación se configura el hardware adjunto al sistema, incluyendo todos los precesadores y los subsistemas de E/S, así como cualquier dispositivo de almacenamiento. A continuación buscará la imagen `initrd` comprimida en una localización predeterminada en memoria, la descomprimirá, la montará y cargará todos los drivers necesarios. A continuación inicializa los dispositivos virtuales relacionados con el sistema de ficheros, tales como LVM o el software de RAID antes de desmontar el la imagen del disco `initrd` y liberar toda la memoria una vez que sea ocupada.

Después de que el kernel haya iniciado todos los dispositivos del sistema, crea un dispositivo de root, monta la partición de root en modo lectura y libera la memoria sin usar.

Llegados a este punto, el kernel está cargado en memoria y operativo. Sin embargo, con aplicaciones que no sean de usuario para dar al usuario la habilidad de proporcionar entrada significativa para el sistema, no se puede hacer mucho más.

Para configurar el entorno de usuario, el kernel inicia el comando `/sbin/init`.

1. Para más detalles sobre como realizar *initrd*, consulte la sección sobre el sistema de ficheros ext3 en el *Manual oficial de personalización de Red Hat Linux*.

3.2.4. Programa `/sbin/init`

El programa `init` coordina el resto del proceso de arranque y configura el entorno para el usuario.

Cuando `init` inicia, se transforma en el padre (o en el abuelo) de todos los procesos que se producen automáticamente en su sistema Red Hat Linux. Primero, pone en funcionamento el guión establecido en el fichero `/etc/rc.d/rc.sysinit`, que establece la ruta a otros programas, activa el swap, controla los sistemas de fichero, etc. Básicamente, el fichero `rc.sysinit` se encarga de todo lo que su sistema tiene que realizar durante la inicialización. La mayor parte de los sistemas usan un reloj, por lo tanto, en ellos, el `rc.sysinit` tendrá una referencia `/etc/sysconfig/clock` para inicializar el reloj. Si tiene procesos especiales en el puerto serie que necesiten ser inicializados, el `rc.sysinit` podría también poner en funcionamiento el `rc.serial`.

El comando `init` ejecuta el script command then runs the `/etc/inittab`, que describe el modo en el que el sistema debería configurarse en cada *runlevel* de *SysV init*. [2]. Entre otras cosas, `/etc/inittab` configura el nivel de ejecución por defecto y dictamina el `/sbin/update` que debe ejecutarse cada vez que se inicie un nivel de ejecución en concreto [3].

A continuación, el comando `init` configura la librería de función de fuente, `/etc/rc.d/init.d/functions`, para el sistema. Esto indica el modo en que empezar o matar un programa y cómo determinar el PID del programa.

El programa `init` inicia todos los procesos de fondo en un directorio `rc` adecuado para el nivel de ejecución especificado como predeterminado `/etc/inittab`. El directorio `rc` está numerado para corresponder al nivel de ejecución que represente. Por ejemplo, `/etc/rc.d/rc5.d/` es el directorio para el nivel de ejecución cinco.

Cuando se arranca el nivel de ejecución 5, el programa `init` consulta el directorio `/etc/rc.d/rc5.d/` para determinar qué procesos iniciar o parar. A continuación un ejemplo de listado para el nivel de ejecución 5, directorio `/etc/rc.d/rc5.d/`:

```
K01pppoe -> ../init.d/pppoe
K05innd -> ../init.d/innd
K10ntpd -> ../init.d/ntpd
K15httpd -> ../init.d/httpd
K15mysqld -> ../init.d/mysqld
K15pvmd -> ../init.d/pvmd
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30mcserv -> ../init.d/mcserv
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K50snmpd -> ../init.d/snmpd
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
```

2. Para obtener más información sobre SysV init, consulte Sección 3.5. Para obtener más información sobre los niveles de ejecución, vaya a Sección 3.6.
3. El comando `update` se usa para eliminar buffers contaminados del disco.

```
K60mars-nwe -> ../init.d/mars-nwe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K75gated -> ../init.d/gated
K80nscd -> ../init.d/nscd
K84ypserv -> ../init.d/ypserv
K90ups -> ../init.d/ups
K96irda -> ../init.d/irda
S05kudzu -> ../init.d/kudzu
S06reconfig -> ../init.d/reconfig
S08ipchains -> ../init.d/ipchains
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S18autofs -> ../init.d/autofs
S20random -> ../init.d/random
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S35identd -> ../init.d/identd
S40atd -> ../init.d/atd
S45pcmcia -> ../init.d/pcmcia
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S60lpd -> ../init.d/lpd
S75keytable -> ../init.d/keytable
S80isdn -> ../init.d/isdn
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90FreeWnn -> ../init.d/FreeWnn
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S95firstboot -> ../init.d/firstboot
S97rhnsd -> ../init.d/rhnsd
S99local -> ../rc.local
S99mdmonitor -> ../init.d/mdmonitor
```

Como puede ver, ningun de los scripts que inician y cierran los servicios están localizados en el directorio. Casi todos los ficheros en `/etc/rc.d/rc5.d/` son *enlaces simbólicos* señalan los scripts localizados en el directorio `/etc/rc.d/init.d/`. Los enlaces simbólicos se usan en cada uno de los directorios `rc` de manera que los niveles de ejecución puedan ser reconfigurados al crear, modificar y eliminar los enlaces simbólicos sin que afecte a los scripts actuales a los que se refiere.

El nombre de cada enlace simbólico con `K` o `S`. Los enlaces `K` son procesos eliminados en ese nivel de ejecución, mientras que aquellos que inician `S`.

El comando `init` para en primer lugar los enlaces simbólicos de `K` en el directorio al ejecutar el comando `/etc/rc.d/init.d/`*`<command>`* `stop` command, en el que *`<command>`* es el proceso a eliminar. A continuación inicia todos los enlaces simbólicos `S` al ejecutar `/etc/rc.d/init.d/`*`<command>`*`. start`.

Advertencia

Una vez que el sistema haya acabado el arranque podrá registrarse como root y ejecutar los mismos scripts para iniciar y parar los servicios. Por ejemplo, el comando paralizará el servidor Web Apache.

Cada uno de los enlaces simbólicos se numera para dictaminar el orden de inicio. Puede cambiar el orden en el que los servicios inician o paran al cambiar el número. Estos enlaces simbólicos con el mismo número se inician de modo alfabético.

En el ejemplo anterior del directorio `/etc/rc.d/rc5.d/`, el comando `init` matará `pppoe`, `innd`, `ntpd`, `httpd`, `mysqld`, `pvmd`, `rarpd`, `bootparamd`, `nfs`, `rstatd`, `rusersd`, `rwalld`, `rwhod`, `squid`, `amd`, `mcserv`, `yppasswdd`, `dhcpd`, `smb`, `vncserver`, `arpwatch`, `named`, `snmpd`, `pxe`, `routed`, `mars-nwe`, `ldap`, `kadmin`, `kprop`, `krb524`, `krb5kdc`, `gated`, `nscd`, `ypserv`, `ups` y `irda`.

Una vez que todos los procesos sean eliminados, `init` busca el mismo directorio y encuentra scripts de inicio para `kudzu`,`reconfig`, `ipchains`, `portmap`, `nfslock`, `autofs`, `random`, `netfs`, `apmd`, `identd`, `atd`, `pcmcia`, `sshd`, `rawdevices`, `xinetd`, `lpd`, `keytable`, `isdn`, `sendmail`, `gpm`, `canna`, `crond`, `FreeWnn`, `xfs`, `anacron` y `mdmonitor`.

La última cosa que el programa `init` lleva a cabo es ejecutar cualquier script localizado en `/etc/rc.d/rc.local` (consulte Sección 3.3 para personalizar `rc.local` file). En este momento, se considera que el sistema está operando en el nivel de ejecución 5.

Después del que el comando `init` haya pasado a través del directorio adecuado `rc` para el nivel de ejecución, el script `/etc/inittab` ejecuta un proceso `getty` para cada consola virtual (intérpretes de comando de registro) ubicada para el nivel de ejecución. Los niveles de ejecución del 2 al 5 obtienen todas las seis consolas virtuales, mientras que el nivel de ejecución 1 (modo usuario único) obtiene tan sólo uno y lo niveles de ejecución son del 0 al 6. El proceso abre las rutas de la comunicación para los dispositivos *tty*. [4], establece sus modos, imprime el indicador de inicio de sesión, toma el nombre del usuario y luego comienza con el proceso de inicio de sesión para ese usuario.

En el nivel de ejecución 5, el `/etc/inittab` ejecuta un guión llamado `/etc/X11/prefdm`. El guión `prefdm` hace funcionar su gestor de pantalla preferido para X (`gdm` si utiliza GNOME o `kdm` si utiliza KDE, basándose en los contenidos del directorio `/etc/sysconfig/desktop`

Para finalizar, el comando `init` ejecuta el script `/etc/rc.d/rc.local`.

3.3. Ejecutar programas en el tiempo de arranque

El script del fichero `/etc/rc.d/rc.local` lo ejecuta el comando `init` en tiempo de arranque, después de que se haya completado toda la inicialización de comandos. Por ejemplo, deseará empezar con demonios adicionales o inicializar una impresora.

Además, si necesita una configuración de puerto serial, podrá crear y modificar `/etc/rc.serial`, y será ejecutado de forma automática en tiempo de arranque. Este script puede ejecutar un número de comandos `setserial` para configurar de manera especial los puertos seriales del sistema. Vaya a la página de manual `setserial` para obtener más información.

3.4. Diferencias en el proceso de arranque de otras arquitecturas

Una vez que el kernel de Red Hat Linux arranca y pasa el proceso de arranque al comando `init`, los mismos acontecimientos suceden en cada arquitectura exactamente en el mismo modo. La única

4. Para mayor información sobre los dispositivos tty, vea la Sección 2.3.10.

diferencia entre el proceso de arranque de cada arquitectura está en la aplicación que se usa para encontrar y cargar el kernel.

Por ejemplo, la arquitectura Alpha usa el gestor de arranque `aboot`, mientras que Itanium usa el gestor de arranque ELILO.

Consulte el Manual oficial de instalación de Red Hat Linux específico para estas plataformas para obtener información detallada sobre la configuración de sus gestores de arranque.

3.5. SysV Init

SysV init es un proceso estándar usado por Red Hat Linux para controlar el software que se lanza para un nivel de ejecución en particular por el comando `init`. Se ha escogido porque es más sencillo de usar y más flexible que el proceso init de estilo BSD.

Los ficheros de configuración para SysV init están en el directorio `/etc/rc.d/` directory. Dentro de este directorio se encuentran los scripts `rc`, `rc.local` y `rc.sysinit`, así como los siguientes directorios:

```
init.d
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
```

El directorio `init.d` contiene los scripts usados por el comando `init` cuando se controlan los servicios. command when controlling services. Each Cada uno de los directorios numerados representa los seis niveles de ejecución predeterminados configurados por defecto bajo Red Hat Linux. Para obtener más información sobre los niveles de ejecución, consulte Sección 3.6.

El nivel de ejecución predeterminado se decide en el fichero `/etc/inittab`. Para averiguar el nivel de ejecución para su sistema, busque una línea similar a que encuentra a continuación al inicio de `/etc/inittab`:

```
id:3:initdefault:
```

El nivel de ejecución predeterminado es tres, como indica el número a continuación de los dos puntos. Si desea cambiarlo, modifique `/etc/inittab` como root.

Warning

Tenga cuidado al modificarlo `/etc/inittab`. Los typos sencillos pueden rovocar que su sistema no pueda arrancarse. Si esto sucediera, necesitará un diskette de arranque para su sistema o introducir el modo rescate para establecer el fichero.

Para obtener más información sobre el modo rescate vea el capítulo que se titula *Modo rescate* del *Manual oficial de personalización de Red Hat Linux*.

3.6. Niveles de ejecución Init

La idea detrás de diferentes sistemas operativos puede ser usada de diversas maneras. Alguno servicios no pueden ser usados hasta que el sistema esté de un determinado modo, o *mode*, como por ejemplo más de un usuario o que tenga disponibilidad de red.

Existen veces en las que desea operar con el sistema en un modo bajo, como por ejemplo al establecer problemas de corrupción de disco en el nivel de ejecución 1, en los que ningún usuario puede estar en el sistema o puede dejar un servidor en un nivel de ejecución 3 sin ejecutar un sesión X. En estos casos, ejecutar servicios que dependan de un modo de sistema más alto para su funcionamiento no tiene sentido porque no funcionarán correctamente de ninguna de las maneras. Teniendo asignado cada servicio para iniciar cuando se alcanza su nivel de ejecución en concreto, le asegura un proceso de arranque ordenado puede cambiar de forma rápida el modo de la máquina sin preocuparse sobre los servicios que inician y paran manualmente.

Generalmente, Red Hat Linux opera en un nivel de ejecución 3 o nivel de ejecución — ambos con modos completos de multi-usuarios. Los siguientes niveles de ejecución están definidos en Red Hat Linux:

- `0` — Parar
- `1` — Modo de usuario único
- `2` — Sin usar (usuario-definible)
- `3` — Modo de multi-usuario completo
- `4` — Sin usar (usuario-definible)
- `5` — Modo de multi-usuario completo(con una pantalla de registro X)
- `6` — Rearrancar

El nivel de ejecución por defecto para que un sistema arranque y se pare está configurado en `/etc/inittab`. Para obtener más información sobre `/etc/inittab`, consulte Sección 3.5.

Si lo desea puede configurar niveles de ejecución 2 y 4. Muchos usuarios configuran aquellos niveles de ejecución en un modo que tiene mucho más sentido y dejan los niveles de ejecución estándar 3 y 5 solos. Esto permite que se muevan en el interior de la configuración personalizada sin interrumpir la configuración normal de las características en los niveles de ejecución estándar.

Si su máquina llega a un punto en el que no arranca debido a un `/etc/inittab` o no le deja registrarse porque posee un `/etc/passwd` o si sencillamente ha olvidado su contraseña, puede arrancar en modo de usuario único.

Si está usando LILO como gestor de arranque, puede arreglar el fichero `inittab` reiniciando el equipo, accediendo al intérprete de comandos `boot:`:

Si está usando GRUB como gestor de arranque, puede arreglar el fichero `inittab` con los siguientes pasos.

- En la pantalla gráfica del gestor de arranque GRUB, seleccione la etiqueta de arranque **Red Hat Linux** y pulse [e] para editarla.
- Pulse la flecha hacia abajo hasta la línea del kernel y presione [e] para editarla.
- En el intérprete de comandos, teclee `single` y pulse [Intro].
- Volverá a la pantalla de GRUB con la información del kernel. Pulse [b] para arrancar el sistema en modo monousuario.

Arrancará un sistema muy escueto y dispondrá de una shell de comandos desde la que puede hacer ajustes.

Si esto no funciona, necesitará arrancar escribiendo **`linux init=/bin/bash`** en el intérprete de comandos de LILO `boot:`. Esto le posiciona en un intérprete de comandos de la shell, observe que ninún sistema de ficheros más que el sistema de ficheros de root está montado y el sistema de ficheros de root está montado sólo en modo lectura. Para montarlo en modo lectura-escritura (para permitir la modificación de `/etc/inittab`, por ejemplo, lleve a cago lo siguiente:

```
mount -n /proc
mount -o rw,remount /
```

3.6.1. Utilidades initscript

La utilidad `/sbin/chkconfig` proporciona una herramienta de línea de comandos sencilla para mantener la jerarquía del directorio `/etc/rc.d/init.d`. Evita que los administradores del sistema tengan que manipular de forma directa los numerosos enlaces simbólicos en los directorios bajo `/etc/rc.d`.

Además, existe `/sbin/ntsysv` que proporciona una interfaz basada en texto mucho más sencilla de usar que la interfaz de la línea de comandos `chkconfig`.

Si prefiere una interfaz gráfica, use el programa **Herramienta de configuración de servicios**, que puede ser invocado usando el comando `redhat-config-services`.

Todas estas utilidades pueden ser ejecutadas como root.

Remítase la capítulo titulado *Control de acceso a servicios* en el *Manual oficial de personalización de Red Hat Linux* para obtener más información relacionada con estas herramientas.

A continuación hablaremos de información dentro de los ficheros de `/etc/sysconfig`, que definen los parámetros usados por los servicios de diferentes sistemas cuando se inicia el sistema.

3.7. Directorio `/etc/sysconfig/`

La información siguiente perfila algunos de los diferentes ficheros de `/etc/sysconfig`, su función y sus contenidos. Esta información no pretende ser completa ya que muchos de estos ficheros permiten una variedad de opciones que se usan sólo en circunstancias muy específicas o raras.

El fichero `/usr/share/doc/initscripts-<`*`version-number`*`>/sysconfig.txt` contiene una lista más autoritaria de los ficheros encontrados en el directorio `/etc/sysconfig` y en las opciones de configuración disponibles.

3.7.1. Ficheros en el `/etc/sysconfig`

Los siguientes ficheros se encuentran normalmente en `/etc/sysconfig`:

- `amd`
- `apmd`
- `arpwatch`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `dhcpd`

- `firstboot`
- `gpm`
- `harddisks`
- `hwconf`
- `i18n`
- `identd`
- `init`
- `ipchains`
- `iptables`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `named`
- `netdump`
- `network`
- `ntpd`
- `pcmcia`
- `radvd`
- `rawdevices`
- `redhat-config-users`
- `redhat-logviewer`
- `samba`
- `sendmail`
- `soundcard`
- `squid`
- `tux`
- `ups`
- `vncservers`
- `xinetd`

Es posible que a su sistema le falten algunos de ellos si el programa que necesita ese fichero no está instalado.

Veamos uno a uno cada uno de estos ficheros.

3.7.1.1. `/etc/sysconfig/amd`

El fichero `/etc/sysconfig/amd` contiene varios parámetros usados por `amd` que permiten montar y desmontar automáticamente los sistemas de ficheros.

3.7.1.2. `/etc/sysconfig/apmd`

El fichero `/etc/sysconfig/apmd` se usa por medio de `apmd` como una configuración para decidir qué iniciar/interrumpir/cambiar en el momento de suspender o reanudar el sistema. Se establece si se va a encender o apagar el ordenador mediante el comando `apmd` durante el inicio, dependiendo de si su hardware soporta *Advanced Power Management* (*APM*) o de que decida usarlo o no. `apm` es un demonio de supervisión que trabaja con el codigo de gestión de energía dentro del kernel Linux. Puede avisarle de una batería descargada si está usando Red Hat Linux en un portátil, entre otras cosas.

3.7.1.3. `/etc/sysconfig/arpwatch`

El fichero `/etc/sysconfig/arpwatch` se usa para pasar argumentos al demonio `arpwatch` durante el arranque del sistema. Este demonio mantien la tabla de direcciones de Ethernet MAC y sus correspondientes direcciones IP. Para mayor información sobre los parámetros que puede usar en este fichero, escriba `man arpwatch`. Por defecto, meste fichero establece como propietario del proceso `arpwatch` al usuario `pcap`.

3.7.1.4. `/etc/sysconfig/authconfig`

El fichero `/etc/sysconfig/authconfig` establece el tipo de autorización que tiene que ser usada en el host. Contiene una o más de las siguientes líneas:

- `USEMD5=<value>`, donde `<value>` puede ser:
  - `yes` — si se usa MD5 para la autenticación.
  - `no` — si no se usa MD5 para la autenticación.
- `USEKERBEROS=<value>`, donde `<value>` puede ser:
  - `yes` — si se usa Kerberos para la autenticación.
  - `no` — si no se usa Kerberos para la autenticación.
- `USELDAPAUTH=<value>`, donde `<value>` es uno de los siguientes valores:
  - `yes` — si LDAP se usa para autenticación.
  - `no` — si LDAP no se usa para autenticación.

3.7.1.5. `/etc/sysconfig/clock`

El fichero `/etc/sysconfig/clock` controla la interpretación de valores leída por el sistema de reloj. Anteriores versiones de Red Hat Linux usaban los siguientes valores (que están anticuados):

- `CLOCKMODE=<value>`, donde `<value>` puede ser:
  - `GMT` — indica que el reloj está regulado con la Hora Universal (Greenwich Mean Time).
  - `ARC` — indica que el período de 42 años de la consola ABC está en funcionamiento (sólo para los sistemas basados en Alpha).

Actualmente, los valores correctos son:

- `UTC=<value>`, donde `<value>` puede ser:

  - `true` — indica que el reloj está regulado con la hora universal. Cualquier otro valor indica que está regulado con la hora local.

- `ARC=<value>`, donde `<value>` puede ser:
  - `true` — indica que el período de tiempo de 42 años de la consola ARC está funcionando. Cualquier otro valor indica que se adopta la norma UNIX epoch (sólo para los sistemas basados en Alpha).

- `ZONE=<filename>` — indica el fichero del huso horario en `/usr/share/zoneinfo` del que `/etc/localtime` es una copia, como:
  `ZONE="America/New York"`

3.7.1.6. `/etc/sysconfig/desktop`

El fichero `/etc/sysconfig/desktop` especifica el gestor de escritorio que va a ser ejecutado, como:

```
DESKTOP="GNOME"
```

3.7.1.7. `/etc/sysconfig/dhcpd`

El fichero `/etc/sysconfig/dhcpd` se usa para pasar argumentos al demonio `dhcpd` durante el procso de arranque el cual implementa los protocolos Dynamic Host Configuration Protocol (DHCP) e Internet Bootstrap Protocol (BOOTP). Estos protocolos asignan nombres de hosts a máquinas de la res. Para mayor información escriba `man dhcpd`.

3.7.1.8. `/etc/sysconfig/firstboot`

Cuando inicia con 8.0, la primera vez que arranque el sistema, el programa `/sbin/init` busca el script `etc/rc.d/init.d/firstboot`. Esto permite que el usuario instale aplicaciones adicionales y documentación antes de que el proceso de arranque sea completado.

El fichero `/etc/sysconfig/firstboot` hace simplemente que no se ejecute el comando `firstboot`. Si desea ejecutar `firstboot` la próxima vez que arranque el sistema, elimine `/etc/sysconfig/firstboot` y ejecute `chkconfig --level 5 firstboot on`.

3.7.1.9. `/etc/sysconfig/gpm`

El fichero `/etc/sysconfig/gpm` se usa para pasar argumentos al demonio `gpm` en el tiempo de arranque. El demonio `gpm` daemon es el servidor de ratón que permite la aceleración del ratón y la tecla del medio. Para obtener más información sobre los parámetros utilice este fichero, escriba `man gpm`. Por defecto, configura el dispositivo del ratón para `/dev/mouse`.

3.7.1.10. `/etc/sysconfig/harddisks`

El fichero `/etc/sysconfig/harddisks` le permitirá configurar su(s) unidad(es) de disco duro. También puede usar `/etc/sysconfig/hardiskhd[a-h]`, para configurar parámetros de discos específicos.

Atención

No haga cambios en este fichero. Si cambia los valores predeterminados cargados aquí, podría dañar toda la información de sus discos duros.

El fichero `/etc/sysconfig/harddisks` puede contener lo siguiente:

- `USE_DMA=1`, si este valor está a 1, se habilita el DMA. Sin embargo, en algunas combinaciones de chipsets y discos duros, el DMA puede causar corrupción de datos. *Verifique la documentación de su disco duro o consulte su fabricante antes de habilitar esta opción.*
- `Multiple_IO=16`, si este valor está a 16, permite la interrupción de E/S a múltiples sectores. Cuando está habilitado, se reduce la sobrecarga del sistema operativo en un 30-50% *Use esta opción con precaución.*
- `EIDE_32BIT=3`, permite el soporte de una tarjeta de E/S tipo (E)IDE 32-bit.
- `LOOKAHEAD=1`, permite una lectura avanzada de la unidad.
- `EXTRA_PARAMS=`, especifica parámetros extra.

3.7.1.11. `/etc/sysconfig/hwconf`

El fichero `/etc/sysconfig/hwconf` hace un listado de todo el hardware que `kudzu` detectó en su sistema, como también de los controladores que se utilizan y de la información relativa al ID del vendedor y de los dispositivos. El programa `kudzu` detecta y configura el hardware nuevo y/o cambiado de un sistema. El fichero `/etc/sysconfig/hwconf` no se puede modificar manualmente. Si lo modifica, los dispositivos podrían aparecer de repente como si hubieran sido cambiados o anulados.

3.7.1.12. `/etc/sysconfig/i18n`

El fichero `/etc/sysconfig/i18n` establece el idioma predeterminado, como:

```
LANG="en_US"
```

3.7.1.13. `/etc/sysconfig/identd`

El fichero `/etc/sysconfig/identd` se usa para pasar argumentos al demonio `identd` durante el arranque. Este demonio devuelve el nombre de usuario de los procesos abiertos con las conexiones TCP/IP. Algunos de los servicios de la red como los servidores FTP e IRC, se quejarán y responderán lentamente si no se ejecuta el comando `identd`. Pero en general, este comando no es necesario de tal manera que si existe algún problema con la seguridad, no lo ejecute. Para mayor información sobre los parámetros que necesita escriba `man identd`. Por defecto, el fichero no contien parámetros.

3.7.1.14. `/etc/sysconfig/init`

El fichero `/etc/sysconfig/init` controla el modo en que el sistema aparecerá y funcionará durante el arranque.

Podrían usarse los siguientes valores:

- `BOOTUP=<value>`, donde `<value>` puede ser:

  - `BOOTUP=color`, significa que activaremos la pantalla estándar en color durante el arranque; donde se muestra, con diversos colores, si se cargan satisfactoriamente o no los dispositivos y los servicios durante el inicio.
  - `BOOTUP=verbose`, significa que activaremos un modo de inicio al modo antiguo, que proporciona mucha más información que el mero mensaje de éxito o fracaso.
  - Cualquier otro valor se traducirá como que queremos utilizar el modo de pantalla normal, sin el juego de caracteres ANSI.

- `RES_COL=<value>`, donde `<value>` es el número de la columna en la pantalla para iniciar etiquetas de estado. Está predeterminado a 60.
- `MOVE_TO_COL=<value>`, donde `<value>` mueve el cursor hacia el valor de la línea `RES_COL`. Se predetermina el eco de salida de las secuencias ANSI con `-e`.
- `SETCOLOR_SUCCESS=<value>`, donde `<value>` configura el color del indicador de éxito. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a verde.
- `SETCOLOR_FAILURE=<value>`, donde `<value>` configura el color utilizado para indicar un fallo. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a rojo.
- `SETCOLOR_WARNING=<value>`, donde `<value>` configura el color utilizado para indicar atención. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a amarillo.
- `SETCOLOR_NORMAL=<value>`, donde `<value>` configura el color 'normal'. Se predetermina el eco de salida de las secuencias ANSI con `-e`.
- `LOGLEVEL=<value>`, donde `<value>` configura el nivel inicial de identificación de la consola para el kernel. El valor por defecto es 7; 8 significa todo (incluso el depurado); 1 significa nada expecto kernel panics. `syslogd` ignorará esto una vez se ejecute.
- `PROMPT=<value>`, donde `<value>` puede tener uno de los siguientes:
  - `yes` — Activa la verificación de teclado para el modo interactivo.
  - `no` — Desactiva la verificación de teclado para el modo interactivo.

3.7.1.15. `/etc/sysconfig/ipchains`

El fichero `/etc/sysconfig/ipchains` contiene información usada por el kernel para configurar el paquete `ipchains` con respecto a las reglas de filtrado de paquetes en el momento del arranque o siempre que el servicio inicie.

Este fichero es modificado ejecutando el comando `/sbin/service ipchains save` cuando hay reglas válidas `ipchains` en su lugar. No debería modificar manualmente este fichero. En vez de ello, use el comando `/sbin/ipchains` para configurar las reglas necesarias del filtrado de paquetes y, a continuación salve las reglas en este fichero mediante el uso de `/sbin/service ipchains save`.

El uso de `ipchains` para configurar las reglas del firewall no se recomienda ya que se ha descartado y desaparecerá en versiones futuras de Red Hat Linux. Si necesita un firewall, debería usar `iptables` en su lugar.

3.7.1.16. `/etc/sysconfig/iptables`

Como `/etc/sysconfig/ipchains`, el fichero `/etc/sysconfig/iptables` guarda información usada por el kernel para proporcionar servicios especializados de filtrado de paquetes en el momento del arranque o en cualquier momento que el servicio inicie.

No debería modificar este fichero a mano a menos que esté familiarizado con los métodos de construcción de reglas `iptables`. Estas reglas son escritas en `/etc/sysconfig/iptables` por el comando `service iptables save`.El modo más sencillo de añadir reglas es usar `/usr/sbin/lokkit` y la aplicación gráfica **gnome-lokkit** para crear su firewall. El uso de estas aplicaciones modificará de forma automática este fichero al final del proceso.

Si lo desea, puede crear de forma manual regla para el uso de `/sbin/iptables` y escribir `/sbin/service iptables save` para añadir las reglas al fichero `/etc/sysconfig/iptables`.

Una vez que exista el fichero, cualquier regla del firewall aquí salvada persistirá a través del sistema de rearranque.

Para obtener más información sobre `iptables` vaya a Capítulo 13.

3.7.1.17. `/etc/sysconfig/irda`

El fichero `/etc/sysconfig/irda` controla cómo están configurados los dispositivos infrarrojos en el arranque del sistema.

Se pueden utilizar los siguientes valores:

- `IRDA=<value>`, donde `<value>` puede tomar uno de los siguiente valores booleanos:
  - `yes` — `irattach` deberá estar en ejecución, para chequear periódicamente si hay algún dispositivo intentando conectarse al puerto infrarrojos, como podría ser el caso de otro portátil intentando una conexión de red. Si va a utilizar dispositivos infrarrojos en su sistema, debería usar este valor.
  - `no` — el programa `irattach` no se ejecutará, evitando la comunicación por infrarrojos.
- `DEVICE=<value>`, donde `<value>` se refiere al dispositivo (normalmente el puerto serie) que maneja las comunicaciones infrarrojas.
- `DONGLE=<value>`, donde `<value>` el tipo de "dongle" que se utiliza para la comunicación en infrarrojos. Esta configuración existe para la gente que utilice "dongles" serie en lugar de puertos infrarrojos reales. Un "dongle" es un dispositivo que se pone en un puerto serie estándar para comunicar mediante infrarrojos. Esta línea está comentada por defecto porque los ordenadores portátiles con puerto infrarrojos son menos comunes que los ordenadores que disponen de "dongles" para simularlo.
- `DISCOVERY=<value>`, donde `<value>` puede tomar uno de los siguientes valores booleanos:
  - `yes` — Inicia `irattach` en modo discovery, que es el modo que chequea en busca de otros dispositivos infrarrojos. Esta opción se tiene que activar para que una máquina busque activamente conexiones infrarrojas (teniendo en cuenta que el otro dispositivo no puede iniciar la conexión).
  - `no` — No inicia `irattach` en modo discovery.

3.7.1.18. `/etc/sysconfig/keyboard`

El fichero `/etc/sysconfig/init` controla el modo en que el sistema aparecerá y funcionará durante el arranque.

Podrían usarse los siguientes valores:

- `BOOTUP=<value>`, donde `<value>` puede ser:

  - `BOOTUP=color`, significa que activaremos la pantalla estándar en color durante el arranque; donde se muestra, con diversos colores, si se cargan satisfactoriamente o no los dispositivos y los servicios durante el inicio.
  - `BOOTUP=verbose`, significa que activaremos un modo de inicio al modo antiguo, que proporciona mucha más información que el mero mensaje de éxito o fracaso.
  - Cualquier otro valor se traducirá como que queremos utilizar el modo de pantalla normal, sin el juego de caracteres ANSI.
- `RES_COL=<value>`, donde `<value>` es el número de la columna en la pantalla para iniciar etiquetas de estado. Está predeterminado a 60.
- `MOVE_TO_COL=<value>`, donde `<value>` mueve el cursor hacia el valor de la línea `RES_COL`. Se predetermina el eco de salida de las secuencias ANSI con `-e`.
- `SETCOLOR_SUCCESS=<value>`, donde `<value>` configura el color del indicador de éxito. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a verde.
- `SETCOLOR_FAILURE=<value>`, donde `<value>` configura el color utilizado para indicar un fallo. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a rojo.
- `SETCOLOR_WARNING=<value>`, donde `<value>` configura el color utilizado para indicar atención. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a amarillo.
- `SETCOLOR_NORMAL=<value>`, donde `<value>` configura el color 'normal'. Se predetermina el eco de salida de las secuencias ANSI con `-e`.
- `LOGLEVEL=<value>`, donde `<value>` configura el nivel inicial de identificación de la consola para el kernel. El valor por defecto es 7; 8 significa todo (incluso el depurado); 1 significa nada expecto kernel panics. `syslogd` ignorará esto una vez se ejecute.
- `PROMPT=<value>`, donde `<value>` puede tener uno de los siguientes:
  - `yes` — Activa la verificación de teclado para el modo interactivo.
  - `no` — Desactiva la verificación de teclado para el modo interactivo.

3.7.1.19. `/etc/sysconfig/kudzu`

El fichero `/etc/sysconfig/kuzdu` le permitirá realizar una prueba segura del hardware de su sistema con `kudzu` en el arranque. Una prueba segura desactiva la prueba del puerto serie.

- `SAFE=<value>`, donde `<value>` puede tomar uno de los siguientes valores:
  - `yes` — `kuzdu` realiza una prueba segura.
  - `no` — `kuzdu` realiza una prueba normal.

3.7.1.20. `/etc/sysconfig/mouse`

El fichero `/etc/sysconfig/mouse` se utiliza para especificar información sobre el ratón disponible. Se pueden usar los siguientes valores:

- `FULLNAME=<value>`, donde `<value>` se refiere al nombre completo del ratón que se está utilizando.

- `MOUSETYPE=<value>`, donde `<value>` puede tener uno de los siguientes valores:
  - `microsoft` — Un ratón Microsoft™.
  - `mouseman` — Un ratón MouseMan™.
  - `mousesystems` — Un ratón Mouse Systems™ mouse.
  - `ps/2` — Un ratón PS/2.
  - `msbm` — Un ratón tipo bus de Microsoft™.
  - `logibm` — Un ratón tipo bus de Logitech™.
  - `atibm` — Un ratón tipo bus de ATI™.
  - `logitech` — Un ratón Logitech™.
  - `mmseries` — Un viejo ratón MouseMan™ mouse.
  - `mmhittab` — Un ratón mmhittab.
- `XEMU3=<value>`, donde `<value>` puede tener uno de los siguientes valores booleanos:
  - `yes` — El ratón tiene sólo dos botones y se quieren emular tres.
  - `no` — El ratón ya tiene tres botones.
- `XMOUSETYPE=<value>`, donde `<value>` se refiere al tipo de ratón que se utilizará mientras se ejecutan las X. Estas opciones son las mismas que las de `MOUSETYPE` en este mismo fichero.
- `DEVICE=<value>`, donde `<value>` es el dispositivo del ratón.

Además, existe un enlace dinámico `/dev/mouse`, que apunta al dispositivo de ratón que se está utilizando actualmente.

3.7.1.21. `/etc/sysconfig/named`

El fichero `/etc/sysconfig/named` se usa para pasar argumentos al demonio `named` daemon durante el arranque. Este demoni es un servidor *Domain Name System* (*DNS*) que implementa la versión 9 de *Berkeley Internet Name Domain* (*BIND*). Este servidor mantiene la tabla de los nombres de hosts que están asociados a las direcciones IP de la red.

Normalmente se usan los siguientes valores:

- `ROOTDIR="</some/where>"`, donde `</some/where>` se refiere al recorrido de todo el directorio de un entorno configurado como chroot en el que se ejecuta `named`. Este entorno tiene que estar configurado. Escriba `info chroot` para mayor informaci^oacute;n.
- `OPTIONS="<value>"`, donde `<value>` representa cualquier opción en la página man de `named` salvo **`-t`**. En vez de **`-t`**, use la línea `ROOTDIR`.

Para mayor información sobre los parámetros que puede usar en este fichero, escriba `man named`. Para saber cómo se configura un servidor BIND DNS, vea el Capítulo 16. Por defecto, el fichero no contiene parámetros.

3.7.1.22. `/etc/sysconfig/netdump`

El fichero `/etc/sysconfig/netdump` es el fichero de configuración del servicio `/etc/init.d/netdump`. El servicio `netdump` manda tanto los satos oops como la memoria a la red. En general, no es necesario usar el servicio `netdump`, por lo que lo debe ejecutar solamente en

caso de absoluta necesidad. Para mayor información sobre los parámetros que puede usar en este fichero, escriba `man netdump`.

3.7.1.23. `/etc/sysconfig/network`

El fichero `/etc/sysconfig/network` se utiliza para especificar información sobre la configuración deseada de la red. Se pueden tener los siguientes valores:

- `NETWORKING=<value>`, donde `<value>` puede tener los siguientes valores booleanos:
  - `yes` — Se debería configurar la red.
  - `no` — No se debería configurar la red.
- `HOSTNAME=<value>`, donde `<value>` debería ser un *Nombre de Dominio Cualificado* (*FQDN*), como pudiera ser `hostname.domain.com`, aunque pudiera ser cualquiera que usted desee.

Nota

Para mantener la compatibilidad con el software antiguo que se pueda tener instalado (como pudiera ser `trn`), el fichero `/etc/HOSTNAME` debería tener el mismo valor que éste.

- `GATEWAY=<value>`, donde `<value>` es la dirección IP de la puerta de enlace de la red.
- `GATEWAYDEV=<value>`, donde `<value>` es el dispositivo de la puerta de enlace, como por ejemplo `eth0`.
- `NISDOMAIN=<value>`, donde `<value>` es el nombre del dominio NIS.

3.7.1.24. `/etc/sysconfig/ntpd`

El fichero `/etc/sysconfig/ntpd` se usa para pasar argumentos al demonio `ntpd` durante el arranque. Este demonio establece y mantiene el sistema hoarario sincronizándolo con un servidor de horas estádar de Internet. Implementa la versión 4 del protocolo Network Time Protocol (NTP). Para mayor información, navegue y busque el fichero `/usr/share/doc/ntp-<version>/ntpd.htm` (donde `<version>` es el número de la versión de `ntpd`). Por defecto, este fichero establece como propietario del proceso `ntpd` al usuario `ntp`.

3.7.1.25. `/etc/sysconfig/pcmcia`

El fichero `/etc/sysconfig/pcmcia` se utiliza para especificar la configuración PCMCIA. Se pueden utilizar los siguientes valores:

- `PCMCIA=<value>`, donde `<value>` se corresponde a uno de los siguientes valores:
  - `yes` — si activamos el soporte de PCMCIA.
  - `no` — si no activamos el soporte PCMCIA.
- `PCIC=<value>`, donde `<value>` se corresponde a uno de los siguientes valores:

- `i82365` — El ordenador tiene un juego de chips PCMCIA de estilo i82365.
- `tcic` — El ordenador tiene un juego de chips PCMCIA de estilo tcic.

- `PCIC_OPTS=<value>`, donde `<value>` corresponde a los parámetros de temporización del driver del socket (i82365 o tcic).
- `CORE_OPTS=<value>`, donde `<value>` es la lista de las opciones `pcmcia_core`.
- `CARDMGR_OPTS=<value>`, donde `<value>` es la lista de las opciones del comando PCMCIA `cardmgr` (como, por ejemplo, `-q` para el modo silencioso; `-m` para buscar módulos del kernel cargables desde un directorio, y demás). Consulte la página de manual sobre `cardmgr` para obtener más información.

3.7.1.26. `/etc/sysconfig/radvd`

El fichero `/etc/sysconfig/radvd` se usa para pasar argumentos al demonio `radvd` durante el arranque. Este demonio escucha las peticiones del router y manda avisos del router para el protocolo IP de la versión 6. Este servicio permite a los hosts de la red cambiara dinámicamente los routers predeterminados basados en estos avisos de router. Para mayor información, escriba `man radvd`. Por defecto, el propietario del proceso `radvd` es el usuario `radvd`.

3.7.1.27. `/etc/sysconfig/rawdevices`

El fichero `/etc/sysconfig/rawdevices` se utiliza para configurar la vinculación de los dispositivos "raw":

```
/dev/raw/raw1 /dev/sda1
/dev/raw/raw2 8 5
```

3.7.1.28. `/etc/sysconfig/redhat-config-users`

El fichero `/etc/sysconfig/redhat-config-users` es el fichero de configuracín de la aplicación gráfica **redhat-config-users**. Bajo Red Hat Linux 8.0 este fichero se usa para filtrar los usuarios del sistema como root, demonio o lp. Este fichero está modificado por el menú despegable **Preferences** => **Filter system users and groups** en la aplicación **redhat-config-users** y no lo debería modificar a mano. Para obtener más información sobre el uso de este aplicación, consulte el capítulo llamado *Configuración de grupo y de usuario* en el *Manual oficial de personalización de Red Hat Linux*.

3.7.1.29. `/etc/sysconfig/redhat-logviewer`

El fichero `/etc/sysconfig/redhat-logviewer` es el fichero de configuración para la aplicación gráfica, de visión de registro interactiva, **redhat-logviewer**. Este fichero está mofificado por el menú despegable **Edit** => **Preferences** en la aplicación **redhat-logviewer** y no debería ser mofificado a mano. Para obtener más información sobre el uso de esta aplicación, consulte el capítulo llamado *Log Files* en el *Manual oficial de personalización de Red Hat Linux*.

3.7.1.30. /etc/sysconfig/samba

El fichero /etc/sysconfig/samba se usa para pasar argumentos a los demonios smbd y nmbd durante el arranque. El demonio smbd permite compartir la conexión de los clientes Windows a la red y el demonio The nmbd ofrece NetBIOS en los servicios IP. Para mayor información escriba man smbd. Por defecto, los deminios se ejecutan en modo demonio.

3.7.1.31. /etc/sysconfig/sendmail

El fichero /etc/sysconfig/sendmail permite que se puedan enviar mensajes a uno o más receptores, enrutando el mensaje sobre tantas redes como sea necesario. Este fichero configura los valores por defecto que la aplicación **Sendmail** necesita para ejecutarse. Estos valores por defecto son para ejecutarlo como un demonio en segundo plano y para verificar la cola una vez cada hora.

Se pueden utilizar los siguientes valores:

- DAEMON=<*value*>, donde <*value*> corresponde a uno de los siguientes valores booleanos:
  - yes — **Sendmail** debería configurarse para escuchar en el puerto 25 a la escucha de correo de entrada. La opción yes implica la utilización de la opción -bd de **Sendmail**.
  - no — **Sendmail** no debería de ser configurado para escuchar la llegada de correo por el puerto 25.
- QUEUE=1h se envía a **Sendmail** como -q$QUEUE. La opción -q no se pasa a **Sendmail** si existe /etc/sysconfig/sendmail y el parámetro QUEUE está vacío o incompleto.

3.7.1.32. /etc/sysconfig/soundcard

El fichero /etc/sysconfig/soundcard es generado por el comando sndconfig y no debería de ser modificado. El único uso de este fichero es determinar qué tarjeta aparecerá por defecto en el menú de selección de sndconfig la próxima vez que se ejecute. La configuración de la tarjeta de sonido se localiza en el fichero /etc/modules.conf.

Este fichero puede contener lo siguiente:

- CARDTYPE=<*value*>, donde <*value*> se configura, por ejemplo, como SB16 en el caso de una tarjeta de sonido Soundblaster 16.

3.7.1.33. /etc/sysconfig/squid

El fichero /etc/sysconfig/squid se usa para pasar argumentos al demonio squid durante el arranque. Este demonio es un servidor proxy caché para las aplicaciones de los cliente de la Web. Para mayor información sobre cómo configuarar un servidor proxy squid, en el navegador abra el directorio /usr/share/doc/squid-<*version*>/ (reemplace <*version*> con el número de la versión de squid instalado en su sistema). Por defecto, este fichero configura el tiempo máximo de arranque de squid en modo demonio y el intervalo de tiempo antes de que se apague.

3.7.1.34. /etc/sysconfig/tux

El fichero /etc/sysconfig/tux es el fichero de configuración del Red Hat Content Accelerator, conocido formalmente como TUX, el servidor de web basado en el kernel. Para mayor informacioacute;n sobre la configuración de TUX, navegue y abra el fichero /usr/share/doc/tux-<*version*>/tux/index.html (reemplace <*version*> con le

número de la versión del TUX instalado en su sistema). Los parámetros de este fichero están en `/usr/share/doc/tux-<version>/tux/parameters.html`.

3.7.1.35. `/etc/sysconfig/ups`

El fichero `/etc/sysconfig/ups` se utiliza para especificar información sobre cualquier *Sistema de Alimentación Ininterrumpida* (*SAI* o *UPS*) conectado a su sistema. Un SAI puede ser una buena opción para un sistema Red Hat Linux ya que le proporcionarát el tiempo necesario para apagar el sistema correctamente en el caso de la interrupción del servicio eléctrico. Se pueden utilizar los siguientes valores:

- `SERVER=<value>`, donde `<value>` puede tomar los siguientes valores:
  - `yes` — Si se ha instalado un SAI en su sistema.
  - `no` — Si no se ha instalado ningún SAI en su sistema.
- `MODEL=<value>`, donde `<value>` debe estar seleccionado a uno de los siguientes valores o bien a `NONE` si no hay ningún SAI instalado en su sistema:
  - `apcsmart` — Para un dispositivo APC SmartUPS™ o similar.
  - `fentonups` — Para un dispositivo Fenton UPS™.
  - `optiups` — Para un dispositivo OPTI-UPS™.
  - `bestups` — Para un SAI Best Power™.
  - `genericups` — Para un SAI genérico.
  - `ups-trust425+625` — Para un SAI Trust™.
- `DEVICE=<value>`, donde `<value>` especifica dónde está conectado el SAI, como pueda ser `/dev/ttyS0`.
- `OPTIONS=<value>`, donde `<value>` es un comando especial que hay que pasarle al SAI.

3.7.1.36. `/etc/sysconfig/vncservers`

El fichero `/etc/sysconfig/vncservers` configura cómo el servidor de *Virtual Network Computing* (*VNC*) se inicia. VNC es un sistema de visualizació remoto que permite visualizar escritorios remotos en otras máquinas diferentes de donde lo estamos ejecutando, pero a través de diferentes redes, (desde una LAN a Internet) usando una variedad de parámetros considerable.

Puede contener lo siguiente:

- `VNCSERVERS=<value>`, donde `<value>` se suele poner com algo parecido a `"1:fred"`, para inidicar que el servidor VNC debe ser lanzado para el usuario fred en el display :1. El usuario fred debe tener una contraseña VNC usando `vncpasswd` antes de intentar conectarse al servidor remoto VNC.

Note que cuando usa un servidor VNC, su comunicación puede estar desencriptada, y esto no debe usarse en una red insegura. Para instrucciones específicas concernientes al uso de SSH para asegurar la comunicación VNC, lea la información encontrada en http://www.uk.research.att.com/vnc/sshvnc.html.

3.7.1.37. `/etc/sysconfig/xinetd`

El fichero `/etc/sysconfig/xinetd` se usa para pasar argumentos al demonio `xinetd` durante el arranque. Este demonio arranca programas que ofrecen servicios de Internet cuando se recibe un a petición en el puerto de escucha. Para mayor información, escriba `man xinetd` y sobre el servicio `xinetd`, vea la Sección 8.3.

3.7.2. Directorios que se encuentran en el directorio `/etc/sysconfig/`

A continuación le mostramos los directorios que se encuentran en `/etc/sysconfig/` y le damos un breve descripción de sus contenidos:

- `apm-scripts` — Contiene el script "suspend/resume" del APM de Red Hat. No debe modificar este fichero directamente. Si necesita la personalizarlo, cree un fichero `/etc/sysconfig/apm-scripts/apmcontinue` que al final será un script. Puede controlar el script modificando el fichero `/etc/sysconfig/apmd`.
- `cbq` — Este directorio contiene los ficheros de configuración que se necsitan para usar Class Based Queuing para administrar la longitud de la banda de los dispositivos de red.
- `networking` — Este directorio lo usa la herramienta **Red Hat Network Administration Tool** pero no se debe modificar a mano. Para mayor información sobre la herramienta **Red Hat Network Administration Tool**, consulte el capítulo *Configuración de la red* en el *Manual oficial de personalización de Red Hat Linux.*
- `network-scripts` — Este directorio contiene los siguientes ficheros de configuración relativos a la red:
  - Ficheros de configuración de la red para cada uno de los dispositivos de red como `ifcfg-eth0` para el dispositivo Ethernet `eth0`.
  - Scripts que se usan para cargar y descargar dispositivos de red como `ifup` y `ifdown`.
  - Scripts que se usan para cargar y descargar dispositivos ISDN como `ifup-isdn` y `ifdown-isdn`
  - Varios scrpits de funciones de la red compartidos que no se deben modificar directamente.

  Para mayor información sobre el directorio `network-scripts` vea el Capítulo 12
- `rhn` — Este directorio contiene los ficheros de configuración de las aplicaciones **Red Hat Network Registration Client**, **Red Hat Update Agent Configuration Tool**, **Red Hat Update Agent** y **Red Hat Network Alert Notification Tool**, así como `systemid` y las claves GPG. No se pueden modificar ficheros en este directorio a mano. Para mayor información sobre la Red Hat Network, vaya a : https://rhn.redhat.com/.

3.8. Apagar

Para apagar Red Hat Linux, ejecute el comando `shutdown`. Puede leer la página del manual de `shutdown` para obtener más detalles, pero los parámetros más usuales son:

```
/sbin/shutdown -h now
/sbin/shutdown -r now
```

Deberá ejecutar `shutdown` como root. Una vez que haya apagado todo, la opción `-h` parará la máquina y la opción `-r` la reiniciará.

Aunque el comando `reboot` y el comando `halt` puedan invocar `shutdown` mientras el sistema se ejecute en los niveles de ejecución 1-5, es una mala costumbre, ya que no todos los sistemas Linux soportan esta opción.

Atención

Si su ordenador no se apaga por sí solo, no deberá apagarlo hasta que no vea un mensaje en la pantalla indicándole que puede hacerlo.

Si se produce un fallo mientras que espera este mensaje, esto quiere decir que lo mismo está intentando apagar su máquina antes de que las particiones de disco hayan sido desmontadas. Esto puede provocar errores en el sistema de ficheros, incluso hasta el punto de no permitirle arrancar el sistema la próxima vez que intente iniciarlo. Tenga paciencia a la hora de apagar su sistema.

Capítulo 4.

Gestores de arranque

Antes de poder ejecutar Red Hat Linux en un sistema, deberá iniciar un programa especial llamado *gestor de arranque*. El programa de gestor de arranque existe en el disco duro primario del sistema o en los dispositivos de medios y es responsable de la carga del kernel de Linux y de los ficheros necesarios, o, en algunos casos, de otros sistemas operativos en la memoria.

4.1. Gestores de arranque y arquitectura del sistema

Cada arquitectura del sistemas que pueda ejecutar Red Hat Linux usa un gestor de arranque diferente. Por ejemplo, la arquitectura Alpha usa el gestor de arranque `aboot`, mientras que la arquitectura Itanium usa el gestor de arranque `ELILO`.

Este capí tulo explica comandos y opciones de configuración para los dos cargadores de arranque con Red Hat Linux 8.0 para la arquitectura x86: GRUB y LILO.

4.2. GRUB

GNU GRand Unified Boot loader o GRUB consiste en un programa que habilita al usuario a seleccionar qué sistema operativo instalado o kernel descargar en el tiempo de arranque del sistema. Permite también que el usuario transmita argumentos al kernel.

4.2.1. Proceso de arranque en un sistema x86 y GRUB

Esta sección explica con más detalle el papel especí fico que desempeña GRUB al arrancar un sistema x86. Para hacerse una idea del proceso de arranque, vea Sección 3.2.

GRUB se carga a sí mismo en la memoria en las diferentes etapas:

1. *La etapa 1 o cargador de arranque primario se lee en la memoria con el BIOS desde el MBR*[1]. El gestor de arranque primario existe en menos de 512 bytes de espacio en disco entre el MBR. Lo único que hace es cargar el gestor de arranque de la etapa 1.5 o la etapa 2.
2. *El gestor de arranque de la etapa 1 lee en la memoria al gestor de arranque de la etapa 1.5.* Determinado hardware requiere un paso intermedio para obtener el cargador de arranque de la etapa 2. Esto sucede a menudo cuando la partición `/boot` está por encima de 1024 cilindros de disco duro o cuando se usa el modo LBA. Este cargador de arranque de la etapa 1.5 se encuentra en la partición `/boot` o en una pequeña parte del MBR y la partición `/boot`.
3. *La etapa 2 o el gestor de arranque secundario se lee en la memoria.* El gestor de arranque secundario visualiza el menú GRUB y el entorno del comando. Esta interfaz le permite seleccionar qué sistema operativo o kernel de Linux arrancar, pasar argumentos al kernel o ver los parámetros del sistema, tales como la RAM disponible.
4. *El gestor de arranque secundario lee el sistema operativo o el kernel y `initrd` en la memoria.* Una vez que GRUB determina qué sistema operativo iniciar, éste lo carga en al memoria y controla la máquina de dicho sistema operativo.

El método de arranque usado para arrancar Red Hat Linux se conoce como método de *carga directa* porque el gestor de arranque carga el sistema operativo directamente. No existe punto medio entre el gestor de arranque y el kernel.

1. Para obtener más información sobre BIOS y el MBR, vaya a Sección 3.2.1.

El proceso de arranque usado por otros sistemas operativos será diferente. Por ejemplo, los sistemas operativos de Microsoft DOS y Windows, así como otros sistemas operativos de propiedad, se cargan mediante el suo de un método de arranque de *carga de cadena*. Bajo este método, el MBR señala el primer sector de la partición al sostener el sistema operativo. A continuación encuentra los ficheros necesarios para arrancar ese sistema operativo.

GRUB soporta ambos métodos de arranque, directo y carga de cadena, permitiendo arrancar desde casi cualquier sistema operativo.

Advertencia

Durante la instalación, la instalación de DOS de Microsoft y Windows sobreescriben completamente el MBR, destruyendo cualquier cargador de arranque ya existente. Si crea un sistema de arranque dual, es preferible que instale el sistema operativo Microsoft en primer lugar. Para obtener instrucciones sobre como llevarlo a cabo, vea el apéndice titulado *Instalación de Red Hat Linux en un entorno de doble arranque* en el *Manual oficial de instalación de Red Hat Linux*.

4.2.2. Funciones de GRUB

GRUB contiene una serie de funciones que lo convierten en el método favorito respecto al resto de gestores de arranque disponibles para la arquitectura x86. A continuación tiene una lista de las caracterí sticas más importantes:

- *GRUB proporciona un entorno pre-OS basado en comandos verdaderos para máquinas x86*. Esto proporciona una flexibilidad máxima en la carga de los sistemas operativos con determinadas opciones o con la recopilación de información sobre el sistema. Durante años muchas arquitecturas que no son x-86 han usado entornos previos al sistema operativo que permiten arrancar el sistema desde una lí nea de comandos. Mientras que algunas caracterí sticas del comando están disponbiles con LILO y otros gestores de arranque para x86, GRUB es una caracterí stica mucho más rica.

  Muchas arquitecturas no basadas en x86 han usado entornos pre-OS durante años que le permiten controlar cómo se arranca el sistema desde una línea de comandos. Aunque algunas funciones de comando están disponibles en LILO y en otros gestores de arranque para x86, GRUB ofrece un número mayor de funciones.

- *GRUB admite el modo Direccionamiento Lógico de Bloques (LBA).*

  El modo LBA inserta la conversión de direccionamiento utilizada para buscar ficheros en la unidad de disco duro del firmware y se utiliza en muchos discos IDE y en todos los discos duros SCSI. Antes de LBA, los cargadores de arranque pueden encontrar la limitación de la BIOS de 1024 cilindros, en la que la BIOS non puede encontrar un fichero tras la cabeza del cilindro del disco. El soporte LBA permite que GRUB arranque los sistemas operativos desde las particiones bajo el lí mite de 1024 cilindros, tan largo cuanto la BIOS del sistema soporta el modo LBA. Las revisiones más modernas de la BIOS soportan el modo LBA.

- *GRUB puede leer las particiones ext2.*. Esto permite que GRUB acceda a su fichero de configuración, `/boot/grub/grub.conf`, cada vez que el sistema arranca, haciendo evidente la necesidad que tiene el usuario de escribir una nueva versión del primer gestor de arranque para el MBR en caso de que se produzcan los cambios de la configuración. El único caso en el que el usuario necesitarí a reinstalar GRUB en el MBR es en caso de que la localización fí sica de la partición `/boot` se traslade al disco. Para más detalles sobre la instalación de GRUB en el MBR, consulte Sección 4.3.

4.3. Instalación de GRUB

Si durante el proceso de instalación de Red Hat Linux no instaló GRUB, a continuación le describimos cómo hacerlo y cómo convertirlo en el gestor de arranque por defecto.

Antes de instalar GRUB, deberí a asegurarse de que cuenta con el último paquete disponible de GRUB desde los CD-ROMs de instalación Red Hat Linux. Para instrucciones sobre los paquetes de instalación, vea el capí tulo titulado *Package Management with RPM* en el *Manual oficial de personalización de Red Hat Linux.*

Once the GRUB package is installed, open a root shell prompt and run the command `/sbin/grub-install <location>`, where <*location*> is the location GRUB Stage 1 boot loader should be installed.

The following command installs GRUB to the MBR of the master IDE device on the primary IDE bus, alos known as the C drive:

```
/sbin/grub-install /dev/hda
```

The next time you boot the system, you should see the GRUB graphical boot loader menu before the kernel loads.

4.4. Terminología de GRUB

Una de las cuestiones más importantes que deben entenderse antes de utilizar GRUB es cómo el programa hace referencia a los dispositivos, por ejemplo, a los discos duros y a las particiones. Esta información es muy importante si desea configurar GRUB para arrancar varios sistemas operativos.

4.4.1. Nombres de dispositivos

GRUB denominará al primer disco duro de un sistema `(hd0)`. A la primera partición de dicho disco, le denominará `(hd0,0)` y a la quinta partición del segundo disco duro `(hd1,4)`. En general, la nomenclatura utilizada para los sistemas de ficheros al usar GRUB se desglosa del siguiente modo:

```
(<tipo-de-dispositivo><número-dispositivo-
bios>,<número-partición>)
```

Los paréntesis y las comas son muy importantes en el nombre. <*tipo-de-dispositivo*> hace referencia a si es un disco duro (`hd`) o una unidad de disquete (`fd`).

<*número-dispositivo-bios*> es el número de dispositivo según la BIOS del sistema, empezando desde `0`. El disco duro IDE principal tiene asignado el número `0` y el disco duro IDE secundario el número `1`. El orden es aproximadamente equivalente al modo en el que el kernel de Linux organiza los dispositivos con letras, donde la letra `a` en `hda` corresponde al número `0`, y la letra `b` en `hdb` corresponde al número `1`, y así sucesivamente.

Nota

El sistema de numeración de GRUB para los dispositivos empieza por `0` y no por `1`. Este es uno de los errores que cometen con más frecuencia los usuarios que empiezan a utilizar GRUB.

<*número-partición*> hace referencia al número de una partición concreta en dicho dispositivo. Al igual que en el caso de <*número-dispositivo- bios*>, la numeración de las particiones empieza por `0`. Aunque la mayoría de las particiones se especifican con números, si el sistema usa particiones BSD a éstas se hará referencia con letras, por ejemplo `a` o `c`.

GRUB usa las reglas siguientes para denominar a los dispositivos y a las particiones:

- No es relevante si los discos duros que utiliza son IDE o SCSI. Todos los discos duros empiezan con `hd`. Las unidades de disquete empiezan con `fd`.
- Para especificar todo un dispositivo sin respetar sus particiones, simplemente debe suprimir la coma y el número de partición. Esto es importante para indicarle a GRUB que configure el registro MBR para un disco concreto. Por ejemplo, `(hd0)` indica el MBR en el primer dispositivo y `(hd3)` especifica el MBR en el cuarto dispositivo.
- Si tiene varios discos duros, es muy importante saber el orden de la unidad de arranque de la BIOS. Esto es muy sencillo si sólo tiene discos IDE o SCSI, pero si tiene una combinación de ambos, el asunto se complica un poco.

4.4.2. Nombres de ficheros

Al escribir comandos en GRUB que hagan referencia a un fichero, como una lista de menús que debe usarse para permitir el arranque de varios sistemas operativos, debe incluir el fichero inmediatamente después de especificar el dispositivo y la partición. Una especificación de fichero de ejemplo que haga referencia a un nombre de fichero absoluto se organiza del modo siguiente:

```
(<tipo-de-dispositivo><número-dispositivo-
bios>,<número-
partición>)/ruta/a/fichero
```

La mayoría del tiempo, deberá especificar ficheros mediante su ruta en esta partición y el nombre de fichero.

También puede especificar ficheros a GRUB que no aparecen realmente en el sistema de ficheros, como un gestor de encadenamiento que se muestra en los primeros bloques de una partición. Para especificar estos ficheros, deberá indicar una *lista de bloques*, que indique a GRUB, bloque por bloque, la ubicación exacta del fichero en la partición. Puesto que un fichero puede estar formado por varios conjuntos de bloques, hay un modo específico de escribir listas de bloques. Cada ubicación de sección de fichero se describe con un número de compensación de bloques seguido de un número de bloques de ese punto de compensación, y las secciones se colocan juntas de forma ordenada y separadas por comas.

Por ejemplo:

```
0+50,100+25,200+1
```

Esta lista de bloques indica a GRUB que debe utilizar un fichero que empieza en el primer bloque de la partición y que usa los bloques del 0 al 49, del 99 al 124, y el 199.

Saber cómo escribir listas de bloques es útil al utilizar GRUB para cargar sistemas operativos que usan el método de carga de encadenamiento, como Microsoft Windows. Puede suprimir el número de compensación de bloques si empieza por el bloque 0. Por ejemplo, el fichero de carga de encadenamiento de la primera partición del primer disco duro tendrá el nombre siguiente:

```
(hd0,0)+1
```

También puede usar el comando `chainloader` con una designación de lista de bloques similar en la línea de comandos de GRUB después de establecer el dispositivo correcto y la partición adecuada como raíz:

```
chainloader +1
```

4.4.3. Sistema de ficheros raíz de GRUB

Algunos usuarios se confunden con el uso del término "sistema de ficheros" en GRUB. Es importante recordar que el sistema de ficheros raíz de GRUB no tiene nada que ver con el sistema de ficheros raíz de Linux.

El sistema de ficheros raíz de GRUB es la partición raíz de un dispositivo concreto. GRUB usa esta información para montar el dispositivo y carga los ficheros desde el mismo.

Con Red Hat Linux, una vez que GRUB ha cargado la partición raíz que contiene el kernel de Linux, que se equipara a la partición `/boot` y contiene el kernel de Linux, el comando `kernel` puede ejecutarse con la localización del fichero del kernel como una opción. Una vez arrancado el kernel inicia, establece su propio sistema de ficheros root. El sistema de ficheros root de GRUB original y los montajes deben olvidarse en este punto; la única finalidad de su existencia era arrancar el fichero del kernel.

Consulte las notas sobre los comandos `root` y `kernel` en la Sección 4.6 para obtener más información.

4.5. Interfaces de GRUB

GRUB dispone de tres eficaces interfaces que proporcionan distintos niveles de funciones. Cada una de estas interfaces le permite arrancar el sistema operativo e incluso pasar de una interfaz a otra dentro del entorno de GRUB.

4.5.1. Interfaz de menú

Si el programa de instalación de Red Hat Linux ha configurado automáticamente GRUB, ésta es la interfaz que ya conoce. En esta interfaz hay un menú de sistemas operativos o kernels preconfigurados con sus propios comandos de arranque en forma de lista ordenada por nombre, después de arrancar el sistema por primera vez. Puede utilizar las teclas de flecha para seleccionar una opción en lugar de la selección por defecto y pulsar la tecla [Intro] para arrancar el sistema. Como alternativa, se puede establecer un período de inactividad, de modo que GRUB inicie la carga de la opción por defecto.

Desde la interfaz de menú, también puede pulsar la tecla [e] para introducir la interfaz del editor de entrada o la tecla [c] para cargar la interfaz de lí nea de comandos.

Consulte la Sección 4.7 para obtener más información sobre la configuración de esta interfaz.

4.5.2. Interfaz del editor de entrada de menú

Para tener acceso a esta interfaz, debe pulsar la tecla [e] en la interfaz de menú. Los comandos de GRUB de dicha entrada se muestran aquí y puede alterar estas líneas de comandos antes de arrancar el sistema operativo si agrega ([o] después de la línea actual; [O] antes de la línea actual), modifica una ([e]) o elimina una ([d]).

Una vez realizados los cambios y cuando las líneas tengan el aspecto deseado, puede pulsar la tecla [b] para ejecutarlas y arrancar el sistema operativo. Con la tecla [Esc] se omiten los cambios y el usuario vuelve a la interfaz de menú estándar. Con la tecla [c] se obtiene acceso a la interfaz de línea de comandos.

4.5.3. Interfaz de línea de comandos

Esta es la interfaz de GRUB más básica, pero también la que proporciona un mayor control. En esta interfaz puede escribir cualquier comando de GRUB seguido de la tecla [Intro] para proceder

a la ejecución correspondiente. Esta interfaz cuenta con algunas funciones similares a las de shell avanzadas, como autocompletar con la tecla [Tab] según el contexto y las combinaciones de teclas con [Ctrl] al escribir comandos, por ejemplo, [Ctrl]-[a] para ir al principio de una línea, y [Ctrl]-[e] para ir al final de una línea. Además, la teclas de flecha, [Inicio], [Fin] y [Supr] funcionan de forma similar al comando `bash` de shell.

Vaya a Sección 4.6, para obtener una lista de comandos comunes.

4.5.4. Orden de uso de interfaces

Cuando el entorno de GRUB se arranca al cargar el gestor de arranque del Nivel 2, busca el fichero de configuración correspondiente. Cuando lo encuentra, lo utiliza para crear la lista de menú de los sistemas operativos y visualiza la interfaz del menú de arranque.

Si no puede encontrar el fichero de configuración o si éste no se puede leer, GRUB lleva al usuario a la interfaz de línea de comandos para que pueda escribir manualmente los comandos necesarios para arrancar un sistema operativo.

En el caso de que el fichero de configuración no sea válido, GRUB imprimirá el error y solicitará la introducción de valores. Esto puede ser muy útil, porque podrá ver con exactitud donde está el problema y corregirlo en el fichero. Si pulsa cualquier tecla, tendrá acceso a la interfaz de menú, donde podrá modificar la opción de menú y corregir el problema según el error que GRUB haya notificado. Si la corrección falla, el error se notifica y puede empezar de nuevo.

4.6. Comandos de GRUB

GRUB permite varios comandos en su lí nea de comandos. Algunos de los comandos aceptan opciones después del nombre y estas opciones deben ir separadas del comando por comas y de otras opciones de esa línea por caracteres de espacio.

En la lista siguiente se indican los comandos más útiles:

- `boot` — Arranca el sistema operativo o gestor de encadenamiento que se ha especificado y cargado previamente.
- `chainloader` *`<nombre-fichero>`* — Carga el fichero especificado como gestor de encadenamiento. Para extraer el fichero en el primer sector de la partición especificada, puede utilizar `+1` como nombre de fichero.
- `displaymem` — Muestra el uso actual de memoria, en función de la información de la BIOS. Esto es útil si no está seguro de la cantidad de RAM que tiene un sistema y todavía tiene que arrancarlo.
- `initrd` *`<nombre-fichero>`* — Le permite especificar un disco RAM inicial para utilizarlo al arrancar. `initrd` es necesario cuando el kernel necesita ciertos módulos para poder arrancar adecuadamente, tales como cuando la partición se formatea con el sistema de ficheros ext3.
- `install` *`<nivel-1>`* *`<instalar-disco>`* *`<nivel- 2>`* p *`<fichero-configuración>`* — Instala GRUB en el registro MBR.

  Advertencia

  Este comando sobrescribirá cualquier información del MBR. Si se ejecuta, cualquier herramienta utilizada para arrancar el sistema operativo que no sea GRUB se perderá.

  Asegúrese de conocer con exactitud lo que está haciendo antes de ejecutar este comando.

  Este comando se puede configurar de distintas maneras. Sin embargo, debe especificar el valor *`<nivel- 1>`*, que representa un dispositivo, una partición y un fichero donde se puede encontrar

la imagen del gestor de arranque principal, por ejemplo `(hd0,0)/grub/stage1`. Además, debe especificar el disco en el que el gestor de arranque del Nivel 1 deberá instalarse, por ejemplo `(hd0)`.

La sección *<nivel-2>* indica al gestor de arranque del Nivel 1 la ubicación del gestor de arranque del Nivel 2, por ejemplo `(hd0,0)/grub/stage2`. La opción `p` Indica al comando `install` que se ha especificado un fichero de configuración en la sección *<fichero- configuración>*, por ejemplo `(hd0,0)/grub/grub.conf`.

- `kernel` *<nombre-fichero-kernel>* *<opción-1>* *<opción- N>* — Especifica el fichero kernel que debe cargarse desde el sistema de ficheros raíz de GRUB cuando se usa la carga directa para arrancar el sistema operativo. Las opciones pueden ir seguidas del comando `kernel`, que se transferirá al kernel al cargarse.

  Para el sistema Red Hat Linux, es probable que tenga una línea similar a la siguiente:
  ```
  kernel /vmlinuz root=/dev/hda5
  ```

  Esta línea especifica que el fichero `vmlinuz` se carga desde un sistema de ficheros raíz de GRUB, por ejemplo, `(hd0,0)`. También se transfiere una opción al kernel que especifica que el sistema de ficheros raíz del kernel del Linux debe encontrarse, al cargarse, en `hda5`,la quinta partición en el primer disco duro IDE. Después de esta opción se pueden insertar varias opciones, si es necesario.
- `root` *<dispositivo-y- partición>* — Configura la partición raíz de GRUB para que sea el dispositivo y la partición concreta, por ejemplo, `(hd0,0)`, y monta la partición de modo que se puedan leer los ficheros.
- `rootnoverify` *<dispositivo-y- partición>* — Realiza la misma función que el comando `root`, pero sin montar la partición.

Hay otros comandos disponibles aparte de los indicados. Escriba `info grub` para obtener una lista completa de los comandos.

4.7. Fichero de configuración de menú de GRUB

El fichero de configuración, usado para crear la lista en la interfaz de menú de GRUB de los sistemas operativos para el arranque, básicamente permite al usuario seleccionar un grupo predefinido de comandos para su ejecución. Pueden utilizarse los comandos que se indican en la Sección 4.6, así como algunos comandos especiales disponibles tan sólo en el fichero de configuración.

4.7.1. Comandos especiales del fichero de configuración

Los comandos siguientes sólo pueden usarse en el fichero de configuración de menú de GRUB:

- `color` *<color-normal>* *<color-seleccionado>* — Le permite configurar los colores específicos que se usarán en el menú. Los dos colores se configuran como color de fondo y de primer plano. Puede usar simplemente los nombres de colores, como `red/black`. Una línea de ejemplo sería similar a la siguiente:
  ```
  color red/black green/blue
  ```
- `default` *<nombre-título>* — Nombre del título por defecto de la entrada que se cargará si se supera el tiempo de actividad de la interfaz de menú.
- `fallback` *<nombre-título>* — Si se utiliza, el nombre de título de la entrada que deberá probarse si falla el primer intento.
- `hiddenmenu` — Si se utiliza, no se podrá mostrar la interfaz de menú de GRUB ni cargar la entrada `default` si caduca el período `timeout`. El usuario puede ver el menú estándar de GRUB si pulsa la tecla [Esc].
- `password` *<contraseña>* — Si se utiliza, el usuario que no conozca la contraseña no podrá modificar las entradas de esta opción de menú.

Opcionalmente, puede especificar un fichero de configuración de menú alternativo después de la `<contraseña>`,de modo que, si se conoce la contraseña, GRUB reiniciará el Nivel 2 del gestor de arranque y utilizará este fichero de configuración alternativo para crear el menú. Si se omite este fichero alternativo del comando, el usuario que sepa la contraseña podrá modificar el fichero de configuración actual.

- `timeout` — Si se utiliza se establece la cantidad de tiempo, en segundos, antes de que GRUB cargue la entrada designada por el comando `default`.
- `splashimage` — Especifica la ubicación de la imagen de pantalla splash que se utilizará al arrancar.
- `title` — Establece el título que se utilizará con un grupo de comandos concreto para cargar un sistema operativo.

El carácter # se puede usar para insertar comentarios en el fichero de configuración de menú.

4.7.2. Estructura del fichero de configuración

El fichero de configuración de GRUB es `/boot/grub/grub.conf`. Los comandos para configurar las preferencias para la interfaz del menú están ubicados al inicio del fichero, seguido de las diferentes entradas para cada sistema operativo o kernels listados en el menú.

El aspecto de un fichero de configuración de menú de GRUB muy básico que permita arrancar el sistema Red Hat Linux o Microsoft Windows 2000 puede ser el siguiente:

```
default= 0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz

# section to load linux
title Red Hat Linux (2.4.18-5.47)
        root (hd0,0)
        kernel /vmlinuz-2.4.18-5.47 ro root=/dev/sda2
        initrd /initrd-2.4.18-5.47.img

# section to load Window 2000
title windows
rootnoverify (hd0,0)
chainloader +1
```

Este fichero indicará a GRUB que cree un menú con Red Hat Linux sistema operativo por defecto y que establezca un arranque automático después de transcurridos 10 segundos. Se proporcionan dos secciones, una para cada entrada de sistema operativo, con comandos específicos para la tabla de partición de cada sistema.

Nota

Observe que está especificado como número por defecto. Esto hace referencia a la primera lí nea `title` con la que GRUB se encuentra. Si desea que `windows` sea predeterminada, cambie el valor de `default=` para **`1`**.

Este capí tulo no abarca la configuración de un fichero de configuración del menú de GRUB para arrancar sistemas operativos múltiples. Consulte Sección 4.11 para obtener información más detallada sobre la configuración de GRUB para arrancar diferentes sistemas operativos.

4.8. LILO

LILO es un acrónimo de *LI*nux *LO*ader y se usado siempre para arrancar linux en sistemas x86 para muchos años. Aunque GRUB es el gestor de arranque por defecto, algunos prefieren usar LILO porque les es más familiar y otros porque GRUB puede causar problemas al arrancar determinado tipo de hardware.

4.8.1. LILO y el proceso de arranque de x86

Esta sección trata en más detalle el rol especí fico que LILO desempeña al arrancar el sistema x86. Para ver con más detenimiento el proceso de arranque, vea Sección 3.2.

LILO se carga a sí mismo en la memoria casi de forma idéntica a GRUB, con la diferencia de que es un gestor de dos etapas.

1. *La etapa 1 o el gestor de arranque primario se lee en al memoria por la BIOS desde el MBR*[2]. El gestor de arranque primario existe en menos de 512 bytes de espacio en disco dentro del MBR. Su función es cargar la etapa 2 del gestor de arranque y pasarle la información de la geometrí a del disco.
2. *La etapa 2 o el gestor de arranque secundario se lee en memoria.*. El gestor de arranque secundario visualiza la pantalla incial de Red Hat Linux. Esta pantalla le permite seleccionar el sistema operativo o el kernel de Linux que desee arrancar.
3. *La etapa 2 lee el sistema operativo o el kernel y lleva a cabo* `initrd` *en memoria.* Una vez que LILO determina qué sistema operativo iniciar, éste lo carga en la memoria y lleva el control de la máquina a ese sistema operativo.

Una vez que se ha llevado a cabo la etapa 2 en memoria, LILO visualiza la pantalla inicial de Red Hat Linux con los diferentes sitemas operativos o kernel que han sido configurados para arrancar. Si posee Red Hat Linux instalado y no ha cambiado nada en el fichero de configuración de LILO, verá tan sólo **linux** como una opción. Si instala el soporte del kernel SMP, verá **linux-up** como una opción. Si ha configurado LILO para arrancar otro sistema operativo, esta pantalla le da la posibilidad de seleccionar qué sistema operativo arrancará. Use las teclas de flechas para evidenciar el sistema operativo y pulse [Enter].

Si desea tener un intérprete de comandos para introducir un comando a LILO, pulse [Ctrl]-[X]. LILO visualiza un intérprete `LILO:` en la pantalla y espera la entrada desde el usuario.

4.8.2. LILO vs. GRUB

En general, LILO funciona de forma parecida a GRUB a excepción de tres diferencias:

- No posee ninguna interfaz del comando interactiva.
- Almacena información sobre la localización del kernel o de si otro sistema operativo se debe cargar en el MBR.
- No puede leer las particiones ext2.

El primer punto significa que el intérprete de comandos para LILO no es interactivo y permite tan sólo un comando con argumentos.

Los últimos dos puntos significan que usted cambia el fichero de configuración de LILO o instala un kernel nuevo, debe reescribir el gestro de arranque LILO de la etapa 1 para el MBR llevando a cabo el comando `/sbin/lilo -v -v`. Este método es más arriesgado que el de GRUB, porque un MBR que no haya sido configurado deja el sistema sin arranque. Con GRUB, si el fichero de configuración

2. Para obtener más información sobre la BIOS del sistema y el MBR, vaya a Sección 3.2.1.

está configurado de forma errónea, será predeterminado simplemente para la interfaz de la lí nea de comandos.

Advertencia

Si actualiza el kernel usando **Red Hat Update Agent**, el MBR será actualizado automáticamente. Para obtener más información sobre RHN, remí tase a la siguiente URL, https://rhn.redhat.comthe MBR will be updated automatically.

4.9. Opciones en `/etc/lilo.conf`

El comando `/sbin/lilo -v -v` accede al fichero de configuración de LILO, `/etc/lilo.conf`, para determinar lo que desea escribir en el MBR. Si desea usar el comando `lilo`, necesitará saber cómo modificar este fichero.

Aviso

Si desea mofificar `/etc/lilo.conf`, asegúrese de que ha hecho una copia de seguridad del fichero antes de cualquier otro cambio. Asegúrese de que posee un disquete de arranque en funcionamiento de manera que sea capaz de arrancar el sistema y realizar cambios en el MBR si existe algún problema. Consulte las páginas de manual para `mkbootdisk` para obtener más información en la creación de un disco de arranque.

`lilo` usa el fichero `/etc/lilo.conf` para determinar qué sistema operativo o kernel iniciar, as í como para saber donde instalarlo (por ejemplo, `/dev/hda` para el primer MBR en el primer disco duro IDE). Un fichero `/etc/lilo.conf` será muy parecido (`/etc/lilo.conf` será un poco diferente):

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
message=/boot/message
lba32
default=linux

image=/boot/vmlinuz-2.4.0-0.43.6
 label=linux
 initrd=/boot/initrd-2.4.0-0.43.6.img
 read-only
 root=/dev/hda5

other=/dev/hda1
 label=dos
```

Este ejemplo le muestra un sistema configurado para arrancar dos sistemas operativos: Red Hat Linux y DOS. A continuación unas cuantas lí neas de este fichero:

- `boot=/dev/hda` advierte a LILO para instalar el primer disco duro en el primer controlador IDE.
- `map=/boot/map` localiza el fichero del mapa. En uso normal, éste deberí a ser modificado.

- `install=/boot/boot.b` hace que LILO instale el fichero especí fico como el nuevo sector de arranque de boot. En un uso normal, esto no deberí a ser alterado. Si falta la lí nea `install`, LILO asumirá `/boot/boot.b` predeterminado como el fichero que se usará.
- La existencia de `prompt` hace que LILO le muestre cualquier cosa que haga referencia a la lí nea `message`. No se le recomienda que elimine la lí nea `prompt`, si la elimina, podrá obtener un intérprete manteniendo pulsada la tecla [Shift] mientras que su máquina empieza a arrancar.
- `timeout=50` configura la cantidad de tiempo que LILO esperará la entrada del usuario antes de proceder con el arranque de la entrada de la lí nea `default`. Esto se mide en décimas de segundo, con 50 por defecto.
- `message=/boot/message` se refiere a la pantalla que LILO visualiza para permitirle seleccionar el sistema operativo o el kernel a arrancar.
- `lba32` describe la geometrí a del disco duro para LILO. Otra entrada común es `linear`. No deberí a cambiar esta lí nea a menos de que sea consciente de lo que está haciendo. De lo contrario, pondrí a su sistema en un estado de no ararnque.
- `default=linux` se refiere al sistema operativo por defecto para LILO para arrancar desde las opciones listadas bajo esta lí nea. El nombre `linux` se refiere a la lí nea `label` en cada una de las opciones de arranque.
- `image=/boot/vmlinuz-2.4.0-0.43.6` esecifica el kernel de linux para arrancar con esta opción de arranque en particular. option.
- `label=linux` nombra la opción del sistema operativo en la pantalla de LILO. En este caso, es también el nombre al que se refiere la lí nea `default`.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` se refiere a la imagen *initial ram disk* que se usa en el tiempo de arranque para inicializar los dispositivos que hacen que el inicio del kernel sea posible. El disco ram inicial es una colección de drivers especí ficos de cada máquina necesarios para operar una tarjeta SCSI, una unidad de disco duro o cualquier otro dispositivo necesario para cargar el kernel. No deberí a intentar compartir los discos ram iniciales entre las máquinas.
- `read-only` especifica que la partición de root (vea `root` line below) sea sólo-lectura y no pueda ser alterada durante el proceso de arranque.
- `root=/dev/hda5` advierte a LILO de la partición del disco a usar como la partición de root.

4.10. Cambiar los niveles de ejecución en el tiempo de arranque

Bajo Red Hat Linux, es posible cambiar el nivel de ejecución por defecto en el tiempo de arranque.

Si usa LILO como su gestor de arranque, acceda al intérprete de comandos al escribir `boot:` [Ctrl]-[X]. A continuación escriba:

`linux` *`number`*

En este comando, reemplace el número *`number`* con el número del nivel de ejecución que desea arrancar de (1 a 5) o la palabra **`single`**.

Si está usanso GRUB como gestor de arranque, siga los pasos siguientes:

- En la pantalla gráfica del gestor de arranque GRUB, seleccione la etiqueta de arranque **Red Hat Linux** y pulse [e] para modificarla.
- Vaya en la parte inferior a la línea del kernel y pulse [e] para modificarla.
- En el intérprete de comandos, escriba el número del nivel de ejecución que desea arrancar de (1 a 5), o la palabra **`single`** y pulse [Enter].
- Volverá a la pantalla de GRUB con la información sobre el kernel. Pulse [b] para arrancar el sistema.

Para obtener más información sobre los niveles de ejecución, consulte Sección 3.6.

4.11. Recursos adicionales

El objetivo de este capítulo sólo es servir de introducción a GRUB y a LILO. Consulte los siguientes recursos para descubrir más cosas sobre cómo funcionan GRUB y LILO.

4.11.1. Documentación instalada

- `/usr/share/doc/grub-0.90` — `/usr/share/doc/grub-0.90` es el directorio que contiene información sobre el uso y la configuración de GRUB.
- La página de información de GRUB, a la que se puede acceder si se escribe el comando `info grub` en el intérprete de comandos, contiene un tutorial, un manual de referencia para el usuario, un manual de referencia para el programador y un documento de Preguntas más frecuentes sobre el GRUB y su uso.
- `/usr/share/doc/lilo-21.4.4` — Este directorio contiene información sobre el uso y la configuración de LILO. En particular, el subdirectorio `doc` contiene un fichero postscript llamado `User_Guide.ps` que da mucha información.

4.11.2. Sitios Web útiles

- http://www.gnu.org/software/grub — Página principal del proyecto GNU GRUB. Este sitio contiene información sobre el estado de desarrollo de GRUB y una sección de Preguntas más frecuentes.
- http://www.uruk.org/orig- grub — Documentación original sobre GRUB antes de que el proyecto se entregue a la Free Software Foundation para su posterior desarrollo.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Multiboot-with- GRUB.html — Investiga los distintos usos de GRUB, incluido el arranque de sistemas operativos que no son Linux.
- http://www.linuxgazette.com /issue64/kohli.html — Artículo de introducción en el que se describe cómo configurar GRUB en el sistema desde el principio y en el que se ofrece una introducción general a las opciones de la línea de comandos de GRUB.
- http://www.tldp.org/HOWTO/mini/LILO.html — Este mini-HOWTO habla de los diferentes usos para LILO, incluyendo los sistemas operativos de arranque diferentes a Linux.

Capítulo 5.

Usuarios y grupos

El control de los *usuarios* y *grupos* está en el núcleo de la administración del sistema de Red Hat Linux.

Los *usuarios* pueden ser gente real (cuentas ligadas a un usuario físico en particular) o usuarios lógicos (cuentas existentes para aplicaciones particulares). Ambos tipos de usuarios, reales o lógicos, tienen un *ID de usuario* (*UID*) y *Group ID* (*GID*).

Los *grupos* son siempre expresiones lógicas de organización. Los usuarios forman grupos y los grupos forman fundaciones de usuarios ligados a los que les dan permisos de lectura, escritura o de ejecución de ficheros.

Cuando se crea un fichero se asigna a un usuario y a un grupo. De la misma manera se asignan la lectura, la escritura y la ejecución de permisos para el propietario del archivo, para el grupo asignado al archivo y para cualquier otro usuario en un host. El usuario y el grupo de un archivo particular, así como los permisos en ese archivo, pueden ser cambiados por un root o, en menor grado, por el creador de un archivo.

Una de las tareas más importantes de cualquier administrador del sistema, es la de gestionar los usuarios y grupos, así como asignar y revocar permisos.

5.1. Herramientas para la creación de usuarios y grupos

La gestión de usuarios y grupos ha sido tradicionalmente tediosa, pero Red Hat Linux posee algunas herramientas y convenciones que facilitan a los administradores su gestión.

De la misma manera que puede utilizar herramientas como `useradd` o `groupadd` para crear un nuevo usuario desde un intérprete de comandos de la shell, una manera bastante conocida de manejar usuarios y grupos es a través de **redhat-config-users**. Consulte el *Manual oficial de personalización de Red Hat Linux* para obtener más información.

En Sección 5.4 se habla sobre los conceptos de permiso y sobre los distintos pasos de la línea de comandos para la gestión de los usuarios.

5.2. Usuarios estándar

En la Tabla 5-1, puede ecntrarse la lista de usuarios estándar creada por el proceso de instalación en el fichero `/etc/passwd`. El ID de grupo (GID) en esta tabla es el *grupo primario* para el usuario. Véase la Sección 5.4 para más información sobre cómo se utilizan los grupos.

Usuario	UID	GID	Directorio principal	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	`/sbin/nologin`
daemon	2	2	`/sbin`	`/sbin/nologin`
adm	3	4	`/var/adm`	`/sbin/nologin`
lp	4	7	`/var/spool/lpd`	`/sbin/nologin`
sync	5	0	`/sbin`	`/bin/sync`

Usuario	UID	GID	Directorio principal	Shell	
shutdown	6	0	/sbin	/sbin/shutdown	
halt	7	0	/sbin	/sbin/halt	
mail	8	12	/var/spool/mail	/sbin/nologin	
news	9	13	/var/spool/news		
uucp	10	14	/var/spool/uucp	/sbin/nologin	
operator	11	0	/root	/sbin/nologin	
games	12	100	/usr/games	/sbin/nologin	
gopher	13	30	/usr/lib/gopher-data	/sbin/nologin	
ftp	14	50	/var/ftp	/sbin/nologin	
nobody	99	99	/	/sbin/nologin	
vcsa	69	69	/dev	/sbin/nologin	
rpm	37	37	/var/lib/rpm	/bin/bash	
wnn	49	49	/var/lib/wnn	/bin/bash	
ntp	38	38	/etc/ntp	/sbin/nologin	
ntp	38	38	/etc/ntp	/sbin/nologin	
nscd	28	28	/	/bin/false	
apache	48	48	/var/www	/bin/false	
mysql	27	27	/var/mysql	/bin/bash	
mailnull	47	47	/var/spool/mqueue	/sbin/nologin	
smmsp	51	51	/var/spool/mqueue	/sbin/nologin	
rpc	32	32	/	/sbin/nologin	
xfs	43	43	/etc/X11/fs	/sbin/nologin	
gdm	42	42	/var/gdm	/sbin/nologin	
rpcuser	29				
nfsnobody	65534				
ident	98				
radvd	75	/	/bin/false		
sshd	74	74	/var/empty/sshd	/sbin/nologin	

Usuario	UID	GID	Directorio principal	Shell	
postgres	26	26	/var/lib/pgsql	/bin/bash	
squid	23	23	/var/spool/squid	/dev/null	
named	25	25	/var/named	/bin/false	
pcap	77	77	/var/arpwatch	/sbin/nologin	
amanda	33	6	var/lib/amanda/	/bin/bash	
mailman	41	41	/var/mailman	/bin/false	
netdump	34	34	/var/crash	/bin/bash	
ldap	55	55	/var/lib/ldap	/bin/false	
postfix	89	89	/var/spool/postfix	/bin/true	
privoxy	100	101	/etc/privoxy		
pvm	24	24	/usr/share/pvm3	/bin/bash	

Tabla 5-1. Usuarios estándar

5.3. Grupos estándar

En la Tabla 5-2, encontrará grupos estándar configurados para el programa de instalación. Los grupos están almacenados en Red Hat Linux en el fichero `/etc/group`.

Group	GID	Members
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	

Group	GID	Members
games	20	
gopher	30	
dip	40	
ftp	50	
lock	54	
nobody	99	
users	100	
slocate	21	
floppy	19	
vcsa	69	
rpm	37	rpm
utmp	22	
wnn	49	
ntp	38	
nscd	28	
apache	48	
mysql	27	
mailnull	47	
smmsp	51	
rpc	32	
xfs	43	
gdm	42	
rpcuser	29	
nfsnobody	65534	
ident	98	
radvd	75	
sshd	74	
postgres	26	
squid	23	
named	25	
pcap	77	
wine	66	
mailman	41	
netdump	34	
ldap	55	

Group	GID	Members
postdrop	90	
postfix	89	
privoxy	101	
pvm	24	

Tabla 5-2. Grupos estándar

5.4. Grupos de usuarios privados

Red Hat Linux utiliza un esquema de *grupo privado de usuario* (*UPG*), que hace que los grupos UNIX sean más fáciles de usar. El esquema UPG no añade ni cambia nada en el modo estándar de UNIX en el manejo de grupos; simplemente ofrece una nueva convención. Siempre que cree un usuario nuevo, por defecto, éste pertenece a un único grupo. El esquema funciona de la siguiente manera:

Grupo de usuario privado

Cada usuario tiene un grupo primario; el usuario es el único miembro del grupo.

umask = 002

La máscara de permisos umask para sistemas UNIX es habitualmente de 022, lo que elimina de la posibilidad de que otros usuarios *y otros miembros del grupo primario del usuario* eliminen ficheros del usuario. Puesto que cada usuario tiene su propio grupo privado en el esquema UPG, esta "protección de grupo" no es necesaria. Una umask de 002 prohibirá a los usuarios modificar ficheros privados de otros usuarios. El valor de umask se asigna en `/etc/profile`

activar el bit setgid en un directorio

Si activa el bit setgid en un directorio (con `chmod g+s` *`directorio`*), los archivos creados en ese directorio tendrán su propio grupo en el grupo del directorio.

En la mayoría de las organizaciones de IT (del inglés Information Technologies) se crea un grupo para cada proyecto y se asigna a la gente a los grupos en los que deben estar. Gestionar los archivos ha sido tradicionalmente difícil, porque cuando alguien crea un archivo, éste pertenece al grupo primario al que pertenezca el creador. Cuando una misma persona trabaja en múltiples proyectos, es difícil asociar un grupo adecuado con los ficheros adecuados. Con el esquema UPG, la asignación de grupos a archivos creados en ese directorio es automática, lo que permite gestionar grupos de proyectos de manera simple.

Suponiendo que estemos ejecutando un proyecto llamado *devel*, con muchos usuarios que modifican los ficheros `devel` en un directorio `devel`. Cree un grupo llamado `devel`, añada el directorio `devel` (`chgrp`) y todos los usuarios del proyecto a `devel`.

Puede añadir un usuario a un grupo usando **redhat-config-users** (consulte el *Manual oficial de personalización de Red Hat Linux*). Si prefiere usar la línea de comandos, utilice `/usr/sbin/groupadd` *`groupname`* command> para crear un grupo. El comando `/usr/bin/gpasswd -a` *`loginname groupname`* añadirá un *`loginname`* de usuario a un grupo. (Consulte `groupadd` y las páginas del manual `gpasswd` si necesita más información sobre sus opciones). El archivo `/etc/group` contiene la información de grupo para su sistema.

Si ha creado el grupo `devel`, ha añadido usuarios al grupo `devel`, cambiado el grupo por el directorio `devel` en el grupo `devel` y activado el bit de setgid para el directorio `devel`, todos los usuarios *devel* serán capaces de conservar su estatus de grupo `devel`, para que otros usuarios *devel* sean capaces de modificarlos.

Si se tienen múltiples proyectos como *devel* y usuarios que trabajan en múltiples proyectos, estos usuarios nunca tendrán que cambiar su umask o grupo cuando cambien de proyecto. El bit setgid en el directorio principal de cada proyecto "selecciona" el grupo adecuado.

Puesto que el directorio home de cada usuario pertenece al usuario y a su grupo privado, es seguro dejar activado el bit setgid en el directorio home del usuario. Sin embargo, por defecto, los archivos se crean con el grupo primario del usuario, así que el bit setgid resulta redundante.

5.4.1. Concepto de grupo privado de usuario

Aunque UPG ha existido en Red Hat Linux desde hace algún tiempo, mucha gente todavía tiene preguntas, tales como, por qué es necesario UPG. Observe el siguiente escenario sin UPG:

- Usted quiere que un grupo de usuarios trabaje en un conjunto de ficheros en, por ejemplo, el directorio `/usr/lib/emacs/site-lisp`. Quiere que unas cuantas personas puedan modificar el directorio. Algunas personas podrán modificar el directorio pero no todas. En primer lugar cree el grupo `emacs`:
  ```
  /usr/sbin/groupadd emacs
  ```
  A continuación, teclee:
  ```
  chown -R root.emacs /usr/lib/emacs/site-lisp
  ```
  para asociar los contenidos del directorio con el grupo `emacs` y añadir los usuarios adecuados al grupo:
  ```
  /usr/bin/gpasswd -a <username> emacs
  ```
- Para permitir a los usuarios crear archivos en el directorio teclee:
  ```
  chmod 775 /usr/lib/emacs/site-lisp
  ```
- Pero cuando un usuario crea un nuevo archivo, se le asigna el grupo del grupo del usuario por defecto (habitualmente `users`). Para evitarlo, teclee:
  ```
  chmod 2775 /usr/lib/emacs/site-lisp
  ```
  que hace que todo lo que se cree en el directorio tenga el grupo "emacs".
- Para que un usuario del grupo emacs pueda modificar un archivo nuevo, es necesario que éste sea creado con permisos 664. Para tal propósito, debe utilizar el umask por defecto 002.
- Todo esto funciona bien, salvo que si su grupo por defecto es `users`, todos los archivos creados en el directorio home del usuario serán sobreescribibles por cualquier miembro del grupo `users` (habitualmente todos los usuarios).
- Para solucionar esto, se hace que cada usuario tenga un "grupo privado" como grupo por defecto.

Llegados a este punto, al hacer la umask 002 por defecto y dar a todo el mundo un grupo privado por defecto, se pueden crear fácilmente grupos de los que los usuarios pueden sacar provecho sin realizar ningún tipo de trabajo extra. Simplemente se crea el grupo y se añaden los usuarios, se ejecuta el comando `chown` y `chmod` en los directorios del grupo.

5.5. Utilidades Shadow

Si está en un entorno multiusuario y no usa un sistema de autentificación de red como Kerberos, debererías considerar el uso de las Utilidades Shadow (también conocidas como *shadow passwords*) para mejorar la protección proporcionada por sus ficheros de autentificación del sistema. Durante la instalación de Red Hat Linux, la protección shadow password para su sistema está activa por defecto, así como *contraseñas MD5* (un método de encriptación de contraseñas alternativo más seguro para almecenarlas en su sistema).

Las contraseñas Shadow ofrecen unas pocas ventajas sobre el estándar previo de almacenaje de contraseñas en sistemas UNIX y Linux, incluyendo:

- Seguridad del sistema mejorada, al mover las contraseñas encriptadas (normalmente localizadas en `/etc/passwd`) a `/etc/shadow`, el cual sólo lo puede leer el root
- Información acerca de vigencias de las contraseñas (cuanto tiempo hace que se cambió por última vez)
- Control sobre cuanto tiempo puede permancer sin cambios una contraseña antes de que el usuario sea obligado a cambiarla.
- La capacidad de usar el fichero `/etc/login.defs` para reforzar la política de seguridad, especialmente a lo concerniente a la vigencia de contraseñas.

El paquete `shadow-utils` contiene una serie de utilidades que soportan:

- Conversión de contraseñas normales a shadow y viceversa (`pwconv`, `pwunconv`)
- Verificación de las contraseñas, grupos, y ficheros shadow asociados (`pwck`, `grpck`)
- Métodos estándar para añadir, borrar y modificar cuentas de usuarios (`useradd`, `usermod`, y `userdel`)
- Métodos estándar para añadir, borrar y modificar grupos de usuarios (`groupadd`, `groupmod`, y `groupdel`)
- Método estándar para administrar el fichero `/etc/group` usando `gpasswd`

Nota

Hay algunos puntos adicionales interesantes que conciernen a estas utilidades:

- Las utilidades funcionarán adecuadamente estén o no activas las utilidades shadow.
- Las utilidades han sido ligeramente retocadas para soportar el uso de grupos privados de usuarios Red Hat. Para una descripción de las modificaciones, vea la página man de `useradd`. Para más información de grupos privados de usuarios, vea la Sección 5.4.
- El script `adduser` ha sido reemplazado con un enlace simbólico a `/usr/sbin/useradd`.
- Las herramientas del paquete `shadow-utils` no están activas para Kerberos, NIS, hesiod, o LDAP. Los nuevos usuarios sólo serán locales. Para más información en Kerberos y LDAP, vea el Capítulo 10 y Capítulo 18.

Capítulo 6.

El sistema X Window

Mientras que el corazón de Red Hat Linux es el kernel, para muchos usuarios, la cara del sistema operativo es el entorno gráfico proporcionando por el *Sistema X Window*, también llamado simplemente *X*.

Este capítulo es una introducción al mundo de detrás del escenario de *XFree86*, la implementación open-source de X que contiene Red Hat Linux.

6.1. El poder de X

Linux comenzó siendo un poderoso sistema operativo basado en servidor, excelente a la hora de procesar programas complejos con altos requisitos de CPU y gestionando cientos o miles de clientes a través de conexiones de red. Gracias a su naturaleza abierta y a su estabilidad, Linux ha evolucionado rápidamente hacia un sistema operativo popular basado en entornos gráficos de usuario para estaciones de trabajo en casa o en la oficina.

En el mundo UNIX™, los entorno de ventanas han existido desde hace décadas, siendo éstos precursores de la mayoría de los utilizados en los sistemas operativos actuales. El sistema X Window es en este momento la interfaz de usuario gráfico (GUI) predominante para sistemas operativos del tipo UNIX.

Para crear este GUI para el usuario, X utiliza una arquitectura que se basa en una relación cliente-servidor. Se inicia un proceso *servidor X* y los procesos *cliente X* se pueden conectar a éste través de la red o bien a través de una interfaz loopback local. El proceso servidor gestiona la comunicación con el hardware, como puede ser con una tarjeta gráfica, un monitor, un teclado o un ratón. El cliente de X existe en el espacio del usuario, realizando peticiones al servidor de X

En los sistemas Red Hat Linux, el servidor XFree86 realiza el rol de servidor de X. Ya que se trata de un proyecto de software open source que se apoya en un gran número de desarrolladores en todo el mundo, XFree86 ofrece un desarrollo rápido, una amplia gama de soporte para diferentes dispositivos y arquitecturas gráficas, así como la posibilidad de ejecutarse en diferentes sistemas operativos y plataformas.

La mayoría de los usuarios de escritorio de Red Hat Linux no tienen que preocuparse del servidor XFree86 que está corriendo en su sistema. Tienen mucho más que aprender sobre su propio entorno de escritorio, en el que pasan la mayoría de su tiempo. El programa de instalación de Red Hat Linux realiza un trabajo excelente de configuración de su servidor XFree86 durante el proceso de instalación, asegurándole que X funcionará de manera óptima desde la primera vez que lo inicie.

El servidor X realiza la mayoría de las tareas difíciles usando una amplia gama de hardware, que requiere una configuración. Si algún aspecto de su sistema cambia, como pueda ser el monitor o la tarjeta gráfica, será necesario volver a configurar XFree86. Además, si está solucionando problemas de XFree86 que no pueden ser resueltos con una utilidad de configuración, como pueda ser **Herramienta de configuración de X** (`redhat-config-xfree86`), puede que necesite acceder su fichero de configuración directamente.

Tip

Herramienta de configuración de X es capaz de configurar XFree86 mientras el servidor X está activo. Para activar el programa de configuración desde la línea de comandos, escriba `redhat-config-xfree86`. Para iniciar **Herramienta de configuración de X** mientras que se encuentra en una sesión activa X, vaya al **Botón de menú principal** (en el panel) => **Herramientas del sistema** => **Mostrar**. Después de usar **Herramienta de configuración de X** durante una sesión X, deberá

desconevtarse de la sesión X actual, y a continuación conectarse de nuevo para que se efectúen los cambios.

6.2. XFree86

Red Hat Linux 8.0 utiliza la versión 4.2 de XFree86 como el sistema X Window de base, que incluye las diversas librerías X necesarias, fuentes, utilidades, documentación y herramientas de desarrollo.

Nota

Red Hat ya no proporciona los paquetes de servidor viejos de la versión 3 de XFree86. antes de actualizar para obtener la última versión de Red Hat Linux asegúrese de que su tarjeta de vídeo es compatible con la versión 4 de XFree86 comprobando la Lista de compatibilidad de hardware Red Hat que se encuentra en esta URL:http://hardware.redhat.com/hcl/.

El servidor X incluye muchas mejoras de última tecnología XFree86 XFree86 como pueden ser el soporte de tarjetas aceleradoras 3D, la extensión XRender para suavizado de fuentes, un diseño basado en controladores modulares, soporte para tarjetas de gráficas y dispositivos de entrada modernos así como otras muchas más características.

El programa de instalación Red Hat Linux instala los componentes base de XFree86. puede instalar cualquier otro paquete opcional XFree86.

El sistema X Window se encuentra principalmente en dos lugares dentro de nuestro sistema de ficheros:

directorio `/usr/X11R6`

Directorio que contiene los binarios del cliente X (directorio `bin`), ficheros de cabecera varios (directorio `include`), librerías (directorio `lib`), páginas del manual (directorio `man`), y documentación variada de X (directorio `>/usr/X11R6/lib/X11/doc/`).

directorio `/etc/X11`

La jerarquía de directorios `/etc/X11/` contiene todos los ficheros de configuración de los diferentes componentes que forman el sistema X Window. Esto incluye los ficheros de configuración para el servidor X en sí, el servidor de fuentes X (xfs), xdm y otros componentes. Los gestores de pantalla, como gdm y kdm, así como los diferentes gestores de ventanas y otras utilidades de X guardan sus ficheros de configuración en esta jerarquía.

XFree86 versión 4 es un único binario ejecutable — `/usr/X11R6/bin/XFree86`. Este servidor carga dinámicamente los diferentes módulos de X en tiempo de ejecución desde `/usr/X11R6/lib/modules`, incluyendo los controladores de vídeo, los controladores del motor de fuentes y otros módulos especiales en función de las necesidades. Algunos de estos módulos se cargan automáticamente mientras que algunos de ellos son opcionales y deberá configurarlos en el fichero de configuración del servidor XFree86 en `/etc/X11/XF86Config` antes de que pueda utilizarlos. Los controladores de vídeo se encuentran en el directorio `/usr/X11R6/lib/modules/drivers`. Los controladores DRI de aceleración de hardware 3D se encuentran en `/usr/X11R6/lib/modules/dri`

6.2.1. Ficheros de configuración del servidor XFree86

Los ficheros del servidor XFree86 se encuentran en el directorio `/etc/X11`. El servidor XFree86 4 utiliza el fichero `/etc/X11/XF86Config`. Cuando se haya instalado Red Hat Linux, se crearán los ficheros de configuración Xfree86 utilizando información compilada durante el proceso de instalación.

Aunque es raro tener que modificar estos ficheros manualmente, siempre es útil conocer las diferentes secciones y los parámetros opcionales que podremos encontrar en ellas.

Cada sección empieza con una línea `Section "<nombre-de-la-seccion>"` y finaliza con una línea `EndSection`. Entre cada una de estas etiquetas encontrará varias líneas que contienen los nombres de las diferentes opciones y al menos un valor por opción (ocasionalmente entre comillas). La siguiente lista explora las secciones más útiles de un fichero de XFree86 4 y los roles de las configuraciones más comunes.

`Device`

Especifica información sobre la tarjeta gráfica que utiliza el sistema. Deberá tener al menos una sección `Device` en su fichero de configuración. Puede tener múltiples secciones `Device` en el caso de disponer de varias tarjetas gráficas o de disponer de múltiples configuraciones que pueden correr en una misma tarjeta. Las siguientes opciones son necesarias o ampliamente utilizadas:

- `BusID` — Especifica la localización del bus de la tarjeta de vídeo. Esta opción solo será necesaria para sistemas con múltiples tarjetas y deberá configurarse de tal forma que la sección `Device` utilice la configuración adecuada para la tarjeta de que se trate.
- `Driver` — Le dice a XFree86 qué controlador de dispositivo deberá utilizar con esta tarjeta de vídeo.
- `Identifier` — Proporciona un nombre único para esta tarjeta de vídeo. Normalmente, este nombre suele ponerse igual que el nombre de la tarjeta usada en esta sección `Device`.
- `Screen` — Configuración opcional utilizada cuando la tarjeta de vídeo tenga más de una *cabeza (head)*, o conector para dar salida a un monitor. Si dispone de múltiples monitores conectados a una misma tarjeta de vídeo, deberá disponer de diferentes secciones `Device`, una por cada valor de `Screen` en cada sección `Device`. El valor que acepta esta opción es un número, empezando por `0` e incrementándose por uno por cada conector de la tarjeta de vídeo.
- `VideoRam` — Cantidad de memoria RAM disponible en la tarjeta de vídeo, en kilobytes. Esta opción no suele ser necesaria, ya que el servidor XFree86 suele probar la tarjeta de vídeo para detectar la cantidad de vídeo RAM disponible. En algunos dispositivos de hardware XFree86 no puede obtener estos valores correctamente, así que esta opción le permite especificar manualmente la cantidad de vídeo RAM de que disponga su tarjeta.

`DRI`

Direct Rendering Infrastructure (DRI) es una interfaz que principalmente permite a las aplicaciones de software en 3D aprovecharse de las ventajas de la aceleración 3D por hardware que poseen las tarjetas de vídeo modernas que se soportan. Además, DRI puede mejorar la aceleración 2D por hardware cuando se utilicen los controladores que hayan sido mejorados con el soporte para operaciones DRI en 2D. Cuando DRI está activado en la sección `Module`, se carga el módulo DRI y se pueden configurar opciones específicas de DRI.

Las tarjetas de vídeo utilizan DRI de diferentes formas. Antes de cambiar cualquiera de los valores de DRI, lea detenidamente el fichero `/usr/X11R6/lib/X11/doc/README.DRI` para obtener información más específica sobre cómo configurar su tarjeta en particular.

`Files`

Dice al servidor XFree86 dónde están los ficheros específicos que se utilizarán cuando se inicie el sistema X Window. Estos ficheros contienen información sobre los servicios particulares que pueden ser necesarios para el servidor. Las opciones más comunes incluyen:

- `FontPath` — Configura el lugar donde el servidor XFree86 puede encontrar fuentes. Se pueden especificar diferentes rutas fijas hacia donde podemos encontrar los ficheros, separadas por comas. Por defecto, Red Hat Linux utiliza `xfs` como servidor de fuentes y apunta `FontPath` hacia `unix/:7100`. Esto le dice al servidor XFree86 que obtenga la información usando sockets de dominio UNIX (UNIX-domain sockets) para el proceso de comunicación (IPC)

  Vea la Sección 6.5 para obtener más información sobre XFree86 y las fuentes.

- `ModulePath` — Le permite configurar múltiples directorios para almacenar los diferentes módulos cargados por el servidor XFree86.

- `RgbPath` — Le dice al servidor XFree86 dónde se encuentra en el sistema de base de datos de color RGB. Esta base de datos es un fichero que define todos los colores válidos en XFree86 y proporciona los valores RGB correspondientes.

`InputDevice`

Configura un dispositivo de entrada como pueda ser un ratón o un teclado para ser utilizado para introducir información en el sistema mediante el servidor XFree86. La mayoría de los sistemas disponen al menos de dos secciones `InputDevice`, una para el teclado, y otra para el ratón. Cada una de estas secciones contiene estas dos líneas:

- `Driver` — Le dice a XFree86 el nombre del controlador que deberá cargar para utilizar este dispositivo.

- `Identifier` — Configura el nombre del dispositivo, normalmente el nombre del dispositivo seguido de un número, empezando con el `0` para el primer dispositivo. Por ejemplo, el primer teclado en `InputDevice` tendrá un valor en `Identifier` de `"Keyboard0"`.

La mayoría de las secciones `InputDevice` contienen líneas que asignan opciones específicas a ese dispositivo. Cada una de estas líneas empieza por `Option` y contiene el nombre de la opción entre comillas, seguido del valor que se quiera asignar a esta opción. Los ratones suelen recibir opciones como `Protocol`, como `PS/2` y `Device`, que especifican qué ratón se usará en esta sección. La sección `InputDevice` está bien comentada, permiténdole configurar opciones adicionales para dispositivos más particulares simplemente eliminando los comentarios de ciertas líneas.

`Module`

Le dice al servidor XFree86 qué módulos de los que se encuentran en el directorio `/etc/X11R6/lib/modules` deberán ser cargados. Los módulos proporcionan al servidor XFree86 funcionalidades adicionales..

Atención

No deberá editar estos valores.

`Monitor`

Se refiere al tipo de monitor utilizado por el sistema. Pueden exisistir varias secciones `Monitor`, una por cada monitor que se quiera utilizar en la máquina, con un mínimo de una sección `Monitor`.

Atención

Tenga cuidado cuando modifique manualmente los valores de las opciones de la sección `Monitor`. Si introduce valores incorrectos en esta sección puede dañar o destruir su monitor. Consulte la documentación que acompañaba su monitor para obtener los parámetros de funcionamiento del mismo.

Las siguientes opciones se suelen configurardurante la instalación o al usar **Herramienta de configuración de X**:

- `HorizSync` — Proporciona a XFree86 el rango de frecuencias de refresco horizontales soportado por el monitor en kHz. Estos valores son usados como referencia por el servidor XFree86 para conocer cómo utilizar un valor en particular de la entrada `Modeline` con este monitor.
- `Identifier` — Proporciona un nombre único para este monitor, normalmente se nombra cada monitor empezando por el `0`. El primer monitor será llamado `"Monitor0"`, el segundo `"Monitor1"`, y así con los demás.
- `Modeline` — Se utiliza para especificar los modos de vídeo que usará el monitor en resoluciones particulares, con ciertas tasas de refresco horizontal y vertical. Las entradas de `Modeline` suelen estar precedidas de un comentario que explica qué es lo que especifica esta línea.

  Si su fichero de configuración no incluye comentarios para las diferentes líneas de los modos, puede escanear los valores (también llamados descripciones de modo) para descubrir qué deberá hacer la línea del modo. Mire la página del manual de `XF86Config` para obtener una explicación detallada sobre la sección de los modos.
- `ModelName` — Parámetro opcional que muestra el nombre del modelo del monitor.
- `VendorName` — Parámetro opcional que muestra el nombre del fabricante del monitor.
- `VertRefresh` — Lista de los rangos de frecuencias de refresco verticales soportados por el monitor, en Hz. Estos valores se usan como referencia para que el servidor XFree86 sepa cuando deberá utilizar cada una de las entradas que aparecen en `Modeline` con este monitor.

`Screen`

Enlaza un `Device` determinado y un `Monitor` que podrán ser utilizados como un par y compartir algunas configuraciones. Deberá tener al menos una sección `Screen` en su fichero de configuración. Las opciones más comunes serían:

- `DefaultDepth` — Le dice a la sección `Screen` la profundidad de color por defecto, en bits. `8` es el valor por defecto, `16` proporciona miles de colores y `32` muestra millones de colores.
- `Device` — Significa el nombre de la sección `Device` que deberá usarse con la sección `Screen`.
- `Identifier` — Identifica la sección `Screen` de tal forma que pueda ser referida por la sección `ServerLayout` y ser utilizada.
- `Monitor` — Es el nombre de la sección `Monitor` que se utilizará con la sección `Screen`.

Puede que tenga sobsecciones de `Display` en la sección `Screen` donde se informe al servidor XFree86 de la profundidad de color (`Depth`) y de la resolución (`Mode`) que deberá probarse antes cuando se esté usando un monitor y una resolución determinados.

`ServerFlags`

Contiene opciones globales varias de XFree86. Estas configuraciones pueden ser sobreescritas por las opciones situadas en la sección `ServerLayout`. Las configuraciones más útiles serían:

- `DontZap` — Previene el uso de la combinación de teclas [Ctrl]-[Alt]-[Retroceso] para finalizar la ejecución del servidor XFree86.

- `DontZoom` — Previene el uso de las combinaciones de teclas [Ctrl]-[Alt]-[Keypad-Plus] y [Ctrl]-[Alt]-[Keypad-Minus] para realizar cambios entre las diferentes resoluciones configuradas.

`ServerLayout`

Enlaza una sección `Screen` con las secciones `InputDevice` así como con varias opciones para crear una colección unificada de preferencias que serán usadas por el servidor XFree86 cuando éste se inicie. Si dispone de más de una sección `ServerLayout` y la que quiere utilizar no está especificada en la línea de comandos cuando se levante el servidor XFree86, la primera sección `ServerLayout` será la que se utilice.

Las siguientes opciones se utilizan en la sección `ServerLayout`:

- `Identifier` — Nombre único que describe esta sección `ServerLayout`.
- `InputDevice` — Nombres de cualquier sección `InputDevice` que se utilizarán con el servidor XFree86. La mayoría de los usuarios tan solo dispondrán de dos líneas aquí, `Keyboard0` y `Mouse0`, el primer teclado y el primer ratón de los configurados en el sistema. Las opciones `CoreKeyboard` y `CorePointer` se refieren al hecho de que éstos son el teclado y ratón preferidos, respectivamente, que se utilizarán con el servidor XFree86.
- `Screen` — Nombre de la sección `Screen` a utilizar. El número a la izquierda del nombre de la sección `Screen` se refiere a un número de pantalla en particular para ser usado en configuraciones con múltiples pantallas. Para tarjetas de vídeo estándar con un solo monitor, este valor será `0`. Los números a la derecha proporcionan las coordenadas absolutas de X e Y para la esquina superior izquierda de la pantalla, por defecto `0 0`.

Para obtener más información, mire la página del manual de `XF86Config`, que contiene una lista detallada de las opciones disponibles.

Para revisar la configuración actual de su servidor XFree86, teclee el comando `xset -q`. Esto le proporcionará información sobre su teclado, dispositivo de puntero, salvapantallas y las rutas de las fuentes.

6.3. Entornos de escritorio y gestores de ventanas

La configuración de un servidor XFree86 no es útil hasta que se accede a ella por un programa cliente X que lo utilizará para mostrar el programa usando el hardware controlado por el servidor X. Los clientes X son programas que han sido diseñados para aprovechar las ventajas del hardware del servidor X así como para proporcionar interactividad con un usuario.

No tiene por qué ejecutar un gestor de ventanas complejo junto con un entorno de escritorio para utilizar aplicaciones clientes de X. Asumiendo que no esté ya en un entorno X y que no tenga un fichero `.xinitrc` en su directorio home, teclee el comando `xinit` para iniciar X con una ventana básica de terminal (la aplicación `xterm` por defecto). Podrá ver que este entorno básico le permite utilizar su teclado, ratón, tarjeta de vídeo y monitor con el servidor XFree86, usando las preferencias del hardware del servidor. Teclee **`exit`** en la línea de comandos de `xterm` para salir de este entorno X básico.

Por supuesto, la mayoría de los usuarios de ordenador requieren más características y utilidades de su entorno gráfico. Los desarrolladores han añadido capas de características para crear entornos interactivo que utilizan todo el poder del servidor XFree86. Estas capas se deviden en dos grupos fundamentatel en función de su propósito.

6.3.1. Gestores de ventanas

Los *gestores de ventanas (Window managers)* son programas clientes de X que pueden controlar cómo se posicionan, cambian de tamaño o se mueven otros programas clientes de X. Los gestores de ventanas pueden también proporcional títulos para las ventanas, foco de teclado o de puntero (ratón), teclas específicas del usuario y redireccionamiento de las acciones de los botones del ratón. Los gestores de ventanas trabajan con una colección de diferentes clientes X, cubriendo los programas de tal forma que le puedan hacer cambiar de aspecto y aparecen en determinados lugares de la pantalla.

En Red Hat Linux 8.0 se incluyen cuatro gestores de ventanas:

- `twm` — El gestor de ventanas minimalista Tab Window Manager, que proporciona el conjunto de utilidades más básico de cualquier otro gestor de ventanas.
- `mwm` — El gestor de ventanas por defecto para el entorno de escritorio GNOME, `mwm` viene de Metacity Window Manager. Es un gestor de ventanas simple y eficiente que soporta los temas del cliente.
- `sawfish` — Este gestor de ventanas completamente caracterizado, era el predeterminado hasta la versión de Red Hat Linux 8.0. Puede usarse con o sin el entorno del escritorio de GNOME.
- `wmaker` — *WindowMaker* Gestor de ventanas completamente caracterizado, diseñado para emular ela apariencia del entorno NEXTSTEP.

Todos estos gestores de ventanas se pueden ejecutar como clientes individuales de X para poder obtener una impresión de sus diferencias. Teclee el comando `xinit <ruta-al-gestor-de-ventanas>` donde `<ruta-al-gestor-de-ventanas>` designa la localización del fichero binario del gestor de ventanas. Este fichero se puede encontrar tecleando `which <nombre-del-gestor-de-ventanas>` o buscando directamente el nombre del gestor de ventanas en un directorio `bin`.

6.3.2. Entornos de escritorio

Un *entorno de escritorio (desktop environment)* une diferentes clientes de X de tal forma que puedan ejecutarse conjuntamente usando métodos similares utilizando un entorno de desarrollo común.

Los entornos de escritorio no son lo mismo que los gestores de ventanas, que tan solo pueden controlar la apariencia y la posición de las ventanas de los clientes de X. Los entornos de escritorio contienen funcionalidades avanzadas que permiten a los clientes de X y otros procesos en ejecución el comunicarse entre sí. Esto permite a todas las aplicaciones escritas para trabajar en ese entorno el integrarse cómodamente y el poder usarse de formas nuevas, como por ejemplo permitiendo arrastrar y dejar texto entre aplicaciones.

GNOME es el entorno de escritorio por defecto en Red Hat Linux. GNOME utiliza el conjunto de herramientas base GTK2 y otros componentes variados que extienden las funcionalidades de base. KDE, otro entorno de escritorio, utiliza otro conjunto de herramientas llamado Qt. Tanto GNOME como KDE contienen aplicaciones avanzadas de productividad, como procesadores de textos, hojas de cálculo y un panel de control que le permitirá configurar completamente el aspecto de su entorno. Ambos entornos pueden ejecutar aplicaciones estándar de X y algunas aplicaciones de KDE pueden ejecutarse en GNOME.

Cuando inicia X utilizando el comando `startx`, se utiliza un entorno de escritorio por defecto. Para cambiar el entorno por defecto que usa X cuando se inicia, abra un terminal y teclee el comando `switchdesk`. Esto abrirá una utilidad gráfica que le permitirá seleccionar el entorno de escritorio o el gestor de ventanas que se utilizará la próxima vez que se inicie X.

Los entornos de escritorio utilizan gestores de ventanas para proporcionar la consistencia de apariencia entre diferentes aplicaciones. KDE contiene su propio gestor de ventanas, llamado `kwm`, especificamente diseñado para realizar esta función.

Para obtener más información sobre la personalización de los entornos de escritorio GNOME y KDE, consulte el *Manual oficial del principiante de Red Hat Linux*.

6.4. Niveles de ejecución

La mayoría de los usuarios ejecutan X a partir de uno de los siguientes niveles de ejecución: 3 o 5. El nivel de ejecución 3 pone al sistema en modo multiusuario con capacidad completa de red. La máquina se iniciará con un login basado en modo texto con todos los servicios preconfigurados para este modo. La mayoría de los servidores se ejecutan en el nivel de ejecución 3, ya que X no es necesario para proporcionar los servicios que requieren la mayoría de los usuarios. El nivel de ejecución 5 es similar al 3, excepto que automáticamente inicia X y proporciona una pantalla de login gráfica. La mayoría de los usuarios de estaciones de trabajo prefieren este método, ya que no les fuerza a ver la línea del intérprete de comandos.

El nivel de ejecución usado por su sistema cuando inicie se puede encontrar en el fichero `/etc/inittab`. Si tiene una línea que se parece a `id:3:initdefault:`, entonces su sistema se iniciará en el nivel de ejecución 3. Si tiene una línea que se parece a `id:5:initdefault:`, su sistema estará configurado para iniciarse en el nivel de ejecución 5. Como usuario root, puede cambiar el número del nivel de ejecución de este fichero y cambiarlo a otro por defecto. Guarde los cambios en el fichero y reinicie su sistema para verificar que se inicia en el nivel de ejecución correcto. Puede encontrar más información sobre los niveles de ejecución en la Sección 3.6.

6.4.1. Nivel de ejecución 3: `startx`

Cuando estamos en nivel de ejecución 3, la forma habitual de iniciar una sesión X es tecleando el comando `startx`. `startx` es un front-end del programa `xinit`, el cual lanza el servidor XFree86 y conecta los clientes X al mismo. Ya que usted debe de haber entrado en el sistema con su usuario cuando realice este procedimiento a partir del nivel de ejecución 3 para poder teclear comandos, `startx` tan solo ha sido diseñado para levantar algunos clientes X, como el entorno de escritorio. No proporciona ninguna autenticación a nivel de usuario.

Cuando `startx` comienza, busca un fichero `.xinitrc` de usuario que se encuentra en el directorio home del mismo para definir qué clientes X se deberán de ejecutar. Si este fichero no se encuentra, se utilizará el script por defecto del sistema, que se encuentra en `/etc/X11/xinit/xinitrc`. El script `startx` realiza la misma operación con el fichero `.xserverrc`, buscándolo en el directorio home del usuario y luego ejecutando el script `/etc/X11/xinit/xserverrc` si no logra encontrarlo. Como existen muchos clientes X diferentes, los ficheros `xinitrc` son muy importantes. El script `xserverrc` es menos importante. Tan solo configura al servidor X para conectarse a los clientes X. Como el servidor X ya está configurado por defecto con el enlace `/etc/X11/X`, Red Hat Linux no instala un `xserverrc` por defecto.

El script `xinitrc` por defecto busca entonces los ficheros definidos por el usuario y los ficheros por defecto del sistema, incluyendo `.Xresources`, `.Xmodmap`, y `.Xkbmap` en el directorio home del usuario y `Xresources`, `Xmodmap`, y `Xkbmap` en el directorio `/etc/X11`. Los ficheros `Xmodmap` y `Xkbmap`, si existen, son usados por la utilidad `xmodmap` para configurar el teclado. Los ficheros `Xresources` se leen para asignar parámetros y valores específicos a aplicaciones particulares.

Una vez configuradas estas opciones, el script`xinitrc` ejecuta todos los scripts que se encuentran en `/etc/X11/xinit/xinitrc.d`. Un script muy importante de los que se encuentran en este directorio es el`xinput`, que configura opciones como el idioma por defecto que se va a utilizar y el entorno de escritorio que se va a iniciar (a partir del fichero `/etc/sysconfig/desktop`).

A continuación, el script `xinitrc` intenta ejecutar `.Xclients` en el directorio home del usuario y se va a `/etc/X11/init/Xclients` si no puede encontrarlo. El objetivo del ficheroXclients es iniciar el entorno de escritorio o, posiblemente, tan solo un gestor de ventanas. El script `.Xclients` del directorio home del usuario inicia el entorno de escritorio específico del usuario o su gestor de

ventanas definido en el fichero `.Xclients-default`. Si el fichero `.Xclients` no existe en el directorio home del usuario, el script standard `/etc/X11/init/Xclients` intentará iniciar otro entorno de escritorio, intentando primero GNOME y luego KDE. Si no se puede encontrar ningún entorno de escritorio, `Xclients` realizará un ciclo de intentos a través de la lista de gestores de ventanas hasta que encuentre uno que se inicie, tras haber intentado cargar el gestor de ventanas por defecto que se encuentra definido en el fichero `.wm_style` del directorio home del usuario.

A partir de este momento, podrá iniciar sus aplicaciones preferidas de X, junto con el servidor XFree86. Si necesita más detalles concerniendo el inicio de X en el nivel de ejecución 3, refiérase a las páginas del manual de los comandos `startx` y `xinit` y lea más información sobre los comandos que se han visto anteriormente.

6.4.2. Nivel de ejecución 5: `prefdm`

El nivel de ejecución 5 utiliza un método diferente para iniciar X. Cuando el sistema se inicia, nadie se ha identificado como usuario en el mismo. Para poder utilizar un usuario e iniciar una sesión, deberán entrar en el sistema mediante el proceso de login. En el nivel de ejecución 5, los usuarios se pueden autenticar utilizando un *gestor de pantalla (display manager)*, un cliente especial de X que permite al usuario introducir su nombre de usuario y su contraseña para poder entrar en el sistema.

En función de los entornos de escritorio instalados en su sistema Red Hat Linux, dispondrá de tres gestores de pantalla que son capaces de manejar la autenticación de los usuarios. El gestor de pantalla **xdm** es la herramienta de autenticación original de X. **xdm** tan solo le permite autenticarse e iniciar una sesión X, nada más. El gestor de pantalla **gdm**, diseñado para trabajar junto al entorno de escritorio GNOME, y el gestor de pantalla **kdm**, usado junto con el entorno de escritorio KDE, le permiten configurar en entorno de escritorio o *sesión (session)*, que podrá utilizar una vez haya realizado la autenticación. Adicionalmente, podrá reiniciar o parar el sistema desde la pantalla de autenticación. El gestor de pantalla `gdm` también le permite cambiar el idioma que podrá utilizar en su sesión X.

Cuando el sistema entra en el nivel de ejecución 5, una línea en el fichero `/etc/inittab` especifica que se ejecuta el script `prefdm` para determinar cuál es el gestor de pantalla preferido para realizar la autenticación del usuario. El script `prefdm` utiliza las preferencias almacenadas en el fichero `/etc/sysconfig/desktop` para encontrar el gestor de pantalla adecuado. Si no se ha especificado ningún entorno de escritorio, `prefdm` intentará realizar un ciclo entre `gdm`, `kdm`, y `xdm` para encontrar uno de ellos y utilizarlo. Una vez que encuentra uno de ellos, `prefdm` lo ejecuta para gestionar la autenticación del usuario.

Cada uno de los gestores de pantalla mira en el fichero `/etc/X11/xdm/Xsetup_0` para configurar la pantalla de bienvenida. Una vez que el usuario haya entrado en el sistema, el script `/etc/X11/xdm/GiveConsole` se ejecuta para asignar la propiedad de la consola al usuario. Entonces, el script `/etc/X11/xdm/Xsession` se ejecuta para realizar la mayoría de las tareas que normalmente ejecuta el script `xinitrc` cuando se inicia X desde el nivel de ejecución 3, incluyendo la preparación del sistema y de los recursos de usuario, así como la ejecución de los scripts del directorio `/etc/X11/xinit/xinitrc.d`.

El usuario puede especificar qué entorno de escritorio quiere utilizar cuando se autentique en el sistema utilizando los gestores de pantalla `gdm` o `kdm` desde el menú **Session**. Si el entorno de escritorio no está especificado en el gestor de pantallas, el script `/etc/X11/xdm/Xsession` buscará los ficheros `.xsession` y `.Xclients` en el directorio home del usuario para decidir qué entorno de escritorio será cargado. Como último recurso, se puede utilizar el fichero `/etc/X11/xinit/Xclients` para seleccionar el entorno de escritorio o el gestor de ventanas que se utilizará, de la misma forma que se hacía en el nivel de ejecución 3.

Cuando el usuario termina su sesión X en la pantalla por defecto (`:0`) y sale de su sesión, se ejecuta el script `/etc/X11/xdm/TakeConsole` y se vuelven a asignar los derechos de propiedad de la consola al usuario root. El gestor de pantalla original, que continúa en ejecución cuando el usuario ha entrado en el sistema, recupera el control del mismo lanzando un nuevo gestor de pantalla. Esto reinicia el servidor XFree86, muestra una nueva ventana de inicio y comienza el proceso una vez más.

Para obtener más información sobre cómo los gestores de pantalla controlan la autenticación de los usuarios, mire la página del manual de `xdm`.

6.5. Fuentes

Red Hat Linux utiliza `xfs` (servidor de fuentes de X - X Font Server) para proporcionar fuentes al servidor XFree86 y a las aplicaciones cliente de X que se encuentren conectadas a él. Aunque es posible el no utilizar `xfs` e indicar las rutas hacia las fuentes en sus ficheros de configuración `XF86Config` y `XF86Config-4`, `xfs` proporciona una serie de ventajas:

- *Es más fácil el añadir y eliminar fuentes, incluso el editar la ruta hacia las mismas.* La *ruta hacia las fuentes* es una colección de rutas en el sistema de ficheros donde se encuentran almacenadas las fuentes. El servicio `xfs` mantiene la ruta de las fuentes independientemente de los ficheros de configuración de XFree86, haciendo mucho más fácil su edición.
- *Las fuentes pueden estar almacenadas en una máquina que actúa como servidor de fuentes, y las fuentes pueden ser compartidas entre múltiples servidores de X a través de la red.* Un conjunto común de fuentes puede mantenerse en un único lugar, y ser compartido fácilmente entre todos los usuarios.
- *Se soportan más tipos de fuentes.* `xfs` puede manejar fuentes TrueType, Type1, y de mapa de bits.

Los ficheros de configuración de XFree86 saben cuándo utilizar `xfs` o las rutas de las fuentes mediante el parámetro de configuración `FontPath` de la sección `Files`. Por defecto, `FontPath` está configurado como `unix/:7100`. Esto le dice al servidor XFree86 que se conecte al puerto 7100 utilizando un enlace de comunicaciones inter-máquina. El servidor `xfs` está escuchando en este puerto y responderá con la información sobre las fuentes cuando el servidor XFree86 lo requiera.

El servicio `xfs` debe estar en ejecución cuando se inicien las X. Si no lo está, será devuelto a la línea del intérprete de comandos, junto con un mensaje de error parecido a `failed to set default font path 'unix/:7100'`. Verifique que `xfs` está en ejecución utilizando el comando `ps aux | grep xfs` . Por defecto, `xfs` está configurado para iniciarse automáticamente en los niveles de ejecución 2, 3, 4 y 5, cubriendo todos los niveles de ejecución que permiten la ejecución del entorno gráfico X. Si `xfs` no se encuentra en ejecución en su sistema, puede iniciarlo como usuario root utilizando el comando `/sbin/service xfs start`. Utilice las utilidades `serviceconf` o `/sbin/chkconfig` para forzar su inicio en los niveles de ejecución correctos. Para mayor información, consulte el capítulo *Acceso al control de los servicios* en el *Manual oficial de personalización de Red Hat Linux*

6.5.1. Configuración de `xfs`

El script `/etc/rc.d/init.d/xfs` inicia el servidor `xfs`. Algunas opciones pueden ser configuradas en el fichero `/etc/X11/fs/config`:

- `alternate-servers` — Configura una lista de servidores alternativos de fuentes que podrán ser utilizados en el caso de que el servidor actual no esté disponible. Los diferentes servidores deberán estar separados por comas.
- `catalogue` — Lista ordenada de rutas que contienen las fuentes a utilizar. Cada ruta hacia las fuentes deberá estar separada por una coma antes de que comience otra nueva ruta en la lista.

  Puede utilizar la cadena `:unscaled` inmediatamente después de la ruta hacia las fuentes para hacer que las fuentes no escalables se carguen antes que el resto de las fuentes de la ruta. Entonces, podrá especificar la ruta completa de nuevo de tal forma que las otras fuentes que sean escalables puedan ser cargadas.
- `client-limit` — Configura el número de clientes que el servidor de fuentes podrá servir antes de comenzar a denegar las conexiones. El número por defecto es `10`.

- `clone-self` — Decide su el servidor de fuentes clonará una nueva versión de sí mismo si se llega al límite definido por el parámetro `client-limit`. Por defecto, esta opción está configurada como `on`. Cambiela a `off` para deshabilitar esta posibilidad.
- `default-point-size` — Configura el tamaño de punto por defecto para cualquier fuente que no especifique este valor. El valor de esta opción está estimado en décimas de puntos. El valor por defecto de `120` se corresponde a fuentes de 12 puntos.
- `default-resolutions` — Especifica una lista de resoluciones soportadas por el servidor XFree86. Cada resolución de la lista debe estar separada por una coma.
- `deferglyphs` — Dice a `xfs` cuando cargar *glyphs*, que en una imagen usada para representar una fuente. Puede desactivar esta posibilidad (`none`), activarla para todas las fuentes (`all`), o activarla solo para las fuentes de 16-bits (`16`), que son las que se suelen utilizar con los idiomas asiáticos.
- `error-file` — Le permite especificar la ruta y el nombre de fichero donde se almacenarán los informes de error de `xfs`.
- `no-listen` — Dice a `xfs` que no escuche utilizando un protocolo en particular. Por defecto, esta opción está configurada con `tcp` para evitar que `xfs` escuche utilizando puertos TCP, por motivos de seguridad. Si planea utilizar xfs para servir fuentes a estaciones de trabajo en red o a una red en sí, deberá borrar el `tcp` de esta línea.
- `port` — Especifica el puerto TCP en el que `xfs` escuchará si el parámetro `no-listen` no existe o está comentado.
- `use-syslog` — Dice a `xfs` que utilice el registro de errores del sistema si está configurado con el valor `on`.

6.5.2. Añadir fuentes

Al usar `xfs`, el proceso de añadir fuentes en su sistema es realmente bastante campechano. Utilice el comando `chkfontpath --list` para ver las rutas hacia fuentes que se encuentran actualmente instaladas en su sistema. Para añadir nuevas fuentes a estos directorios, siga las instrucciones que le exponemos a continuación, como usuario root:

1. Cree un directorio para las fuentes, como pueda ser `/usr/share/fonts`, y sitúe las fuentes en el interior del mismo. Asegúrese de cambiar los permisos correctamente; tan solo es necesario que los ficheros se puedan leer, cualquier otro permiso no es necesario.
2. Teclee el comando `chkfontpath --add` *`<directorio-de-fuentes>`*, donde *`<directorio-de-fuentes>`* es la ruta completa al directorio donde las fuentes se encuentren. Esto añadirá esta ruta al fichero de configuración de `xfs`.

Nota

Deberá tener un fichero `fonts.dir` en su nuevo directorio para que el comando `chkfontpath` pueda trabajar correctamente. La creación del fichero `fonts.dir`, así como de otros ficheros utilizados por `xfs` con esas fuentes está más allá del objetivo de este documento.

Muchas de las colecciones de fuentes disponibles para Linux incluyen este fichero, y no será necesario que lo creemos a mano.

3. Reinicie `xfs` utilizando el comando`service xfs restart`. Necesitará también reiniciar su sesión X.
4. Si teclea el comando `chkfontpath --list`, verá la nueva ruta hacia las fuentes. Todas las fuentes que haya aádido al nuevo directorio estarán ahora disponibles para ser utilizadas.

El sitio de soporte de Red Hat contiene más información sobre este tema, mire la págna http://www.redhat.com/support para obtener documentos adicionales de ayuda.

6.6. Recursos adicionales

Se podría decir mucho más sobre el servidor XFree86, los clientes que se conectan a él y la variada gama de entornos de escritorio y gestores de ventanas. Los usuarios avanzados interesados en trucar su configuración de XFree86 pueden encontrar la información de los recursos adicionales bastante útil para lograr sus objetivos.

6.6.1. Documentación instalada

- `/usr/X11R6/lib/X11/doc` — Describe brevemente la arquitectura de XFree86 y cómo obtener información adicional sobre el proyecto XFree86 como nuevo usuario.
- `/usr/X11R6/lib/X11/doc/README.Config` — Explica las opciones de configuración avanzada abiertas para usuarios de Xfree86 3.
- `README.Config` — Explica las opciones de configuración avanzadas disponibles para la versión 3 de XFree86 users.
- `man XF86Config` — Contiene información sobre los ficheros de configuración XFree86, incluyendo el significado y la sintaxis para las diversas secciones dentro de los ficheros.
- `man XFree86` — El manual primario para tod la información de XFree86, detalla la diferencia entre conexiones de servidor X locales y de red, explora variables de entorno comunes, enumera opciones de líneas de comandos y proporciona combinaciones clave administrativas de gran ayuda.
- `man Xserver` — Describe el servidor de pantalla X.

6.6.2. Sitios web útiles

- http://www.xfree86.org — Página principal del proyecto XFree86, que presenta la versión open source del sistema X Window. XFree86 se proporciona junto con Red Hat Linux para proporcionar el control sobre el hardware necesario y proporcionar un entorno gráfico de usuario.
- http://dri.sourceforge.net — Página principal del proyecto DRI (Direct Rendering Infrastructure). DRI es el corazón del componente de aceleración 3D de XFree86.
- http://www.redhat.com/mirrors/LDP/HOWTO/XFree86-HOWTO — Un documento COMO (HOWTO) detallando cómo realizar la instalación manual y la configuración personalizada de XFree86.
- http://www.gnome.org — Página principal del proyecto GNOME, en entorno de escritorio por defecto de XFree86 utilizado en Red Hat Linux.
- http://www.kde.org — Página principal del entorno de escritorio KDE, donde podrá encontrar la última información y documentación.

6.6.3. Libros relacionados

- *The Concise Guide to XFree86 for Linux* de Aron Hsiao; Que — Proporciona un punto de vista experto sobre la operación de XFree86 en sistemas Linux.

- *The New XFree86* de Bill Ball; Prima Publishing — Discute XFree86 y su relación con los entornos de escritorio más populares, como GNOME y KDE.
- *Beginning GTK+ and GNOME* de Peter Wright; Wrox Press, Inc. — Introduce a los programadores la arquitectura de GNOME, mostrando cómo iniciarse con GTK+.
- *GTK+/GNOME Application Development* de Havoc Pennington; New Riders Publishing — Una visión avanzada del corazón de la programación en GTK+, centrándose en código de ejemplo a través de una visión de las APIs disponibles.
- *KDE 2.0 Development* de David Sweet y Matthias Ettrich; Sams Publishing — Instruye a los programadores principiantes y avanzados sobre cómo sacarle partido a las diferentes guías de entorno necesarias para construir aplicaciones para KDE.

Seguridad

Capítulo 7.

Pluggable Authentication Modules (PAM)

Los programas que ofrecen privilegios a los usuarios deben autentificar (verificar la identidad) adecuadamente cada usuario. Al iniciar una sesión en un sistema, el usuario proporciona su nombre de usuario y contraseña y el procedimiento de inicio de sesión usa el nombre de usuario y la contraseña para verificar su identidad.

Los *Módulos de autenticación conectables (PAM)* permiten que al administrador de sistema establezca una política de autenticación sin tener que recompilar programas de autenticación. Con PAM, se controla cómo determinados módulos de autenticación se conectan a un programa editando el fichero de configuración PAM de ese programa en el directorio `/etc/pam.d`.

La mayoría de los usuarios de Red Hat Linux nunca necesitarán modificar los ficheros de configuración de PAM para ninguno de sus programas. Siempre que use RPM para instalar programas que requieren una autentificación, se producirán cambios automáticamente necesarios para la autentificación de la contraseña normal. Sin embargo, si necesita personalizar el fichero de configuración PAM, deberá entender la estructura de este fichero (consulte Sección 7.2 para más información).

7.1. Las ventajas de PAM

Cuando se usa correctamente, PAM aporta muchas ventajas para un administrador de sistema, entre ellas:

- Un esquema de autenticación común que se puede usar con una gran variedad de aplicaciones.
- Permite gran flexibilidad y control de la autentificación para el administrador del sistema y el desarrollador de la aplicación.
- Los desarrolladores de aplicaciones no necesitan desarrollar su programa para usar un determinado esquema de autenticación. En su lugar, pueden concentrarse puramente en los detalles de su programa.

7.2. Ficheros de configuración PAM

El directorio `/etc/pam.d` contiene los ficheros de configuración de PAM. En versiones antiguas de PAM se utilizaba `/etc/pam.conf`. El fichero `pam.conf` todavía se lee si no se encuentran entradas `/etc/pam.d/`, pero se desaprueba su uso.

Cada aplicación (o *servicio*, como se conocen comúnmente las aplicaciones proyectadas para ser usadas por muchos usuarios) tiene su propio fichero dentro del directorio `/etc/pam.d/`.

Estos ficheros tienen una presentación específica que contiene llamadas a los módulos habitualmente localizados en el directorio `/lib/security/`. Adicionalmente, cada línea dentro de un fichero de configuración PAM debe especificar un tipo de módulo, una bandera de control, una ruta hacia el módulo, y, en ocasiones, argumentos del módulo.

7.2.1. Nombres de servicio de PAM

El nombre de servicio de todas las aplicaciones habilitadas para PAM es el nombre de su fichero de configuración en `/etc/pam.d`. Cada programa que usa PAM define su propio nombre de servicio.e instala el fichero de configuración PAM en el directorio `pam.d`. Por ejemplo, el programa `login` define el nombre del servicio como `/etc/pam.d/login`.

Generalmente, el nombre de servicio es el nombre del programa usado para obtener *acceso* al servicio, no del programa usado para *proporcionar* el servicio. Este es el motivo por el que el servicio `wu-ftpd` define su nombre de servicio como `/etc/pam.d/ftp`.

Las próximas cuatro secciones describen el formato básico de los ficheros de configuración de PAM y muestran cómo usan los módulos PAM para ejecutar la autentificación para las aplicaciones que soportan PAM.

7.3. Módulos PAM

Existen cuatro tipos de módulos PAM usados para controlar el acceso a los servicios. Estos tipos establecen una correlación entre los diferentes aspectos del proceso de autorización:

- `auth` — proporcionan la autenticación en sí (tal vez pidiendo y controlando una contraseña) y establecen las credenciales, como la afiliación de grupo o los billetes de Kerberos.
- `account` — controlan que la autenticación sea permitida (que la cuenta no haya caducado, que el usuario tenga permiso de iniciar sesiones a esa hora del día, etc.).
- `password` — se usan para establecer contraseñas.
- `session` — se usan después de que un usuario ha sido autentificado. Los módulos `session` permiten que alguien use su cuenta (para armar el directorio de inicio del usuario o poner a disposición su buzón electrónico, por ejemplo).

Nota

Un módulo individual puede direccionar más de uno de los tipos de módulos mencionados anteriormente. Por ejemplo, `pam_unix.so` tiene componentes que direccionan los cuatro.

En un fichero de configuración PAM, el tipo de módulo es el primer aspecto a definir. Por ejemplo, una línea típica de en una configuración sería: like this:

```
auth      required  /lib/security/pam_unix.so
```

Esto provoca que PAM observe el componente `auth` del módulo `pam_unix.so`.

7.3.1. Apilar módulos

Estos módulos se pueden *apilar*, o colocar uno sobre otro para que se puedan usar los módulos múltiples. El orden de una pila de módulos es muy importante en el procedimiento de autenticación.

El hecho de apilarlos hace que sea más fácil para el administrador exija diversas condiciones antes de permitir la autentificación del usuario. Por ejemplo, `rlogin` normalmente usa cinco módulos `auth`, como se puede ver en el fichero de configuración de PAM:

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
```

Antes de que a alguien se le permita llevar a cabo el `rlogin`, PAM verifica que el fichero `/etc/nologin` no exista, que no esté intentando iniciar una sesión en modo remoto como root y

que se pueda cargar cualquier variable de entorno. Entonces se lleva a cabo una autenticación `rhosts` exitosa antes que se permita la conexión. Si falla la autenticación `rhosts`, entonces se lleva a cabo una autenticación de contraseña estándar.

7.3.2. Creación de módulos

Se pueden añadir módulos PAM nuevos en cualquier momento y después se pueden crear aplicaciones que se puedan usar con los módulos de PAM. Si por ejemplo usted crea un método de creación de contraseñas para usarse una sola vez y escribe un módulo PAM que lo soporte, los programas conscientes de PAM pueden usar el módulo nuevo y el método para contraseñas inmediatamente sin tener que ser recompilados o modificados. Como podrá imaginar, esto es muy positivo, porque le permite combinar y emparejar, además de probar, los métodos de autenticación muy rápidamente con programas diferentes sin tener que recompilar los programas.

La documentación sobre la escritura de módulos contenida en el sistema se encuentra en el directorio `/usr/share/doc/pam-`*`version-number`*`>/`.

7.4. Los indicadores de control PAM

Todos los módulos PAM generan un resultado de éxito o fracaso cuando se les hace un control. Los indicadores de control le dicen a PAM qué hacer con el resultado. Como los módulos pueden apilarse en un determinado orden, los indicadores de control le dan la posibilidad de fijar la importancia de un módulo con respecto a los módulos que lo siguen.

Una vez más, considere el fichero de configuración PAM `rlogin`:

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
```

Importante

El orden en el que se nombran los módulos `required` no es crítico. Los indicadores `sufficient` y `requisite` hacen que el orden sea importante. Consulte más abajo para una explicación de cada tipo de indicador.

Después de que se especifique el tipo de módulo, los indicadores de control deciden la importancia con la que debería ser considerado ese determinado tipo de módulo en cuanto al propósito general de permitirle a ese usuario el acceso a ese programa.

El estándar PAM define cuatro tipos de indicadores de control:

- Los módulos `required` indicados deben ser controlados con éxito para que se permita la autenticación. Si fracasa el control de un módulo `required`, el usuario no recibirá un aviso hasta que no hayan sido controlados los demás módulos del mismo tipo.
- Los módulos `requisite` indicados también deben ser controlados con éxito para que la autenticación sea exitosa. Sin embargo, si fracasa un control de módulo `requisite`, el usuario recibe un aviso inmediatamente con un mensaje que refleja el primer módulo `required` *o* `requisite` fracasado.

- Si fracasan los controles a módulos `sufficient` indicados, se ignoran. Pero si un módulo `sufficient` indicado pasa el control con éxito y ningún módulo `required` indicado antes de ese ha fracasado, entonces ningún otro módulo de este tipo se controlará y el usuario será autenticado.
- Los módulos `optional` indicados no son esenciales para el éxito o fracaso general de la autenticación para ese tipo de módulo. Desempeñan un papel sólo cuando ningún otro módulo de ese tipo ha tenido éxito o ha fallado. En este caso el éxito o fracaso de un módulo `optional` indicado determina la autenticación PAM general para ese tipo de módulo.

Ya está a disposición para PAM una sintaxis de indicador de control más nueva que permite más control. Consulte la documentación de PAM ubicada en `/usr/share/doc/pam-`*`version-number`*`/` para obtener más información sobre esta sintaxis nueva.

7.5. Rutas de módulos PAM

Las rutas de los módulos le indican a PAM dónde encontrar el módulo conectable que hay que usar con el tipo de módulo especificado. Generalmente, se proporciona como una ruta entera de módulo, como `/lib/security/pam_stack.so`. Sin embargo, si no se proporciona la ruta entera (o sea que la ruta no inicia con `/`), entonces se supone que el módulo indicado está en `/lib/security`, la ubicación por defecto para los módulos PAM.

7.6. Argumentos PAM

PAM utiliza argumentos para transmitir información a un módulo conectable durante la autenticación para ese determinado tipo de módulo. Estos argumentos permiten que los ficheros de configuración PAM para determinados programas utilicen un módulo PAM común pero en maneras diferentes.

Por ejemplo, el módulo `pam_userdb.so` utiliza los secretos almacenados en un fichero Berkeley DB para autentificar al usuario. (Berkeley DB es un sistema de base de datos de open source proyectado para ser incrustado en muchas aplicaciones para rastrear determinados tipos de información.) El módulo toma un argumento `db`, especificando el nombre de fichero Berkeley DB que hay que usar, el cual puede variar según el servicio.

La línea `pam_userdb.so` en un fichero de configuración PAM sería más o menos así:

```
auth      required  /lib/security/pam_userdb.so db=path/to/file
```

Los argumentos inválidos se ignoran y no afectan en ningún modo el éxito o fracaso del módulo PAM. Cuando pasa un argumento inválido, el error normalmente se escribe en `/var/log/messages`. Sin embargo, como el método de informe está controlado por el módulo PAM, depende del módulo registrar el error correctamente.

7.7. Muestras de ficheros de configuración PAM

A continuación una muestra de fichero de configuración de la aplicación PAM:

```
#%PAM-1.0
auth      required  /lib/security/pam_securetty.so
auth      required  /lib/security/pam_unix.so shadow nullok
auth      required  /lib/security/pam_nologin.so
account   required  /lib/security/pam_unix.so
password  required  /lib/security/pam_cracklib.so retry=3
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
session   required  /lib/security/pam_unix.so
```

La primera línea es un comentario como toda línea que inicie con el carácter # . Las líneas dos, tres y cuatro apilan tres módulos a usar para autentificaciones de inicio de sesión.

```
auth      required  /lib/security/pam_securetty.so
```

La segunda línea se asegura de *si* el usuario está intentando el registro como root, el tty en el que se están registrando está listado en el fichero `/etc/securetty`, *si* éste existe.

```
auth      required  /lib/security/pam_unix.so nullok
```

Esta línea provoca que se le exija una contraseña al usuario y comprueba la contraseña mediante eluso de la información almacenada en `/etc/passwd` y, de existir, `/etc/shadow`. El módulo `pam_unix.so` dertecta de forma automática y usa las contraseñas shadow almacenadas en `/etc/shadow` para autentificar los usuarios. Remítase a Sección 5.5 para más información sobre las contraseñas shadow.

El argumento `nullok` provoca que el módulo `pam_unix.so` permita una contraseña en blanco.

```
auth      required  /lib/security/pam_nologin.so
```

Este es el último paso de autentificación. Controla si el fichero `/etc/nologin` existe. Si existe `nologin` y el usuario no es root, la autentificación no funcionará.

Note

Note que se controlan los tres módulos `auth`, *no importa si falla el primer módulo* `auth`. Esta estrategia no permite que el usuario se dé cuenta de por qué no se ha permitido su autenticación. Dicha información en manos de un atacador no podría permitir que saquearan el sistema.

```
account   required  /lib/security/pam_unix.so
```

Esta línea conlleva la verificación de la cuenta. Por ejemplo, si las contraseñas shadow han sido habilitadas, el componente de la cuenta del módulo `pam_unix.so` comprobará si la cuenta ha expirado o si el usuario no ha cambiado sus contraseñas dentro del período permitido.

```
password  required  /lib/security/pam_cracklib.so retry=3
```

Si una contraseña ha expirado, el componente de la contraseña del módulo `pam_cracklib.so` le pedirá una nueva contraseña. Pruebe la contraseña de nueva creación para ver si ésta puede ser fácilmente determinada por un programa que descubre las contraseñas de diccionario. Si falla dicha prueba la primera vez, el usuario recibe dos oportunidades más para crear una contraseña más robusta debido al argumento `retry=3`.

```
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
```

Esta línea especifica que si el programa cambia la contraseña del usuario, éste debería usar el componente `password` del módulo `pam_unix.so` para realizarlo. Esto sucederá tan sólo si la porción `auth` del módulo`pam_unix.so` ha determinado que la contraseña necesita ser cambiada — por ejemplo, si una contraseña shadow ha expirado.

El argumento `shadow` hace que el módulo cree contraseñas shadow cuando se actualiza la contraseña del usuario.

El argumento `nullok` indica al módulo que permita al usuario cambiar su contraseña *desde* una contraseña en blanco, de lo contrario se crea una contraseña vacía como bloqueo de cuenta.

El argumento final de esta línea `use_authtok` proporciona un buen ejemplo de cómo se pueden apilar los módulos PAM. Este argumento advierte al módulo a no indicar al usuario una nueva contraseña. En su lugar se acepta cualquier contraseña que pase a través de módulos de contraseña anteriores. De este modo todas las contraseñas nuevas deben pasar el test `pam_cracklib.so` para contraseñas seguras antes de que sean aceptadas.

```
session required /lib/security/pam_unix.so
```

La última línea especifica que el componente de la sesión del módulo `pam_unix.so` gestionará la sesión. Este módulo registra el nombre de usuario y el tipo de servicio para `/var/log/messages` al inicio y al final de cada sesión. Puede ser suplementado apilándolo con otros módulos de sesión si necesita más funcionalidad.

El siguiente ejemplo revisará la configuración `auth` para `rlogin`:

```
#%PAM-1.0
auth      required    /lib/security/pam_nologin.so
auth      required    /lib/security/pam_securetty.so
auth      required    /lib/security/pam_env.so
auth      sufficient  /lib/security/pam_rhosts_auth.so
auth      required    /lib/security/pam_stack.so service=system-auth
```

En primer lugar, `pam_nologin.so` comprueba si `/etc/nologin` existe. Si lo hace, nadie se podrá registrar salvo root.

```
auth      required    /lib/security/pam_securetty.so
```

El módulo `pam_securetty.so` evita que el registro de root se produzca en terminales inseguras. Esto niega el permiso a todos los intentos de `rlogin` de root por motivos de seguridad. Si necesita registrarse como root, utilice en su lugar OpenSSH.

```
auth      required    /lib/security/pam_env.so
```

El módulo carga las variable de entorno especificadas en `/etc/security/pam_env.conf`.

```
auth      sufficient  /lib/security/pam_rhosts_auth.so
```

Los módulos `pam_rhosts_auth.so` autentifican al usuario mediante el uso de `.rhosts` en el directorio principal del usuario. Si esto sucede, PAM autentifica inmediatamente la sesión `rlogin`. Si `pam_rhosts_auth.so` no puede autentificar al usuario, se ignorará este intento de autentificación.

```
auth      required    /lib/security/pam_stack.so service=system-auth
```

Si falla el módulo `pam_rhosts_auth.so` para autentificar el usuario, el módulo `pam_stack.so` ejecuta la autentificación de la contraseña de forma normal.

El argumento `service=system-auth` significa que el usuario deberá pasar a través de la configuración de PAM para la autorización del sistema encontrado en `/etc/pam.d/system-auth`.

Nota

Si no desea que se pida la contraseña cuando el control `securetty` fracasa y determina que el usuario está intentando iniciar una sesión a nivel de root en modo remoto, puede cambiar el módulo `pam_securetty.so` de `required` a `requisite`.

7.8. PAM y propiedad del dispositivo

Red Hat Linux permite que el primer usuario con privilegios que se registre en la consola física de la máquina la habilidad de manipular dispositivos y ejecutar tareas normalmente reservadas para el usuario root. Esto se realiza a través de un módulo PAM llamado `pam_console.so`.

7.8.1. Propiedad del dispositivo

Cuando un usuario se registra en una máquina bajo Red Hat Linux, el módulo `pam_console.so` adquiere el nombre de `login` o del programa gráfico **gdm**. Si este usuario es el primer usuario en registrarse en la consola física — llamado *console user* — el módulo concede la propiedad de una variedad de dispositivos que normalmente posee root. El usuario de la consola posee estos dispositivos hasta que la última sesión local para ese usuario finaliza. Una vez que el usuario se ha desconectado, la propiedad de los dispositivos vuelve a los valores por defecto.

Los dispositivos afectados incluyen, pero no son limitados, las tarjetas de sonido, las unidades de disco y las unidades de CD-ROM.

Esto permite que el usuario local manipule estos dispositivos sin llegar a root, de manera que se simplifican las tareas comunes para el usuario de la consola.

Puede modificar la lista de dispositivos controlados por `pam_console.so` en el fichero `/etc/security/console.perms`.

7.8.2. Acceso de la aplicación

También se permite el acceso a cualquier programa con un fichero qeu soporte el nombre de comando en el directorio `/etc/security/console.apps/`. Estos ficheros no necesitan contener ningún dato, pero deben tener el nombre exacto del comando al que corresponden.

Un grupo notable de aplicaciones a las que tiene acceso el usurario de la consola son tres programas que cierran o abren el sistema. Estos son:

- /sbin/halt
- /sbin/reboot
- /sbin/poweroff

Ya que existen aplicaciones que soportan PAM, éstas llaman `pam_console.so` como requisito para el uso.

Para más información vea las páginas de manual para `pam_console`, `console.perms` y `console.apps`.

7.9. Recursos adicionales

Para obtener mucha más información sobre PAM puede remititirse a diferentes fuentes de información que le servirán de gran ayuda a la hora de configurar PAM en su sistema.

7.9.1. Documentación instalada

- páginas de manual `pam` — buena información introductoria sobre PAM, incluyendo la estructura y propósito de los ficheros de configuración PAM.

- `/usr/share/doc/pam-<version-number>` — contiene excelente documentación en HTML sobre PAM, además de la *Manual para administradores de sistema*, un *Manual para escritores de módulos* y un *Manual para desarrolladores de aplicaciones* . También contiene una copia del estándar PAM, DCE-RFC 86.0.

7.9.2. Sitios web útiles

- http://www.kernel.org/pub/linux/libs/pam — el sitio web principal de distribución para el proyecto Linux-PAM, contiene información sobre varios módulos y aplicaciones PAM actualmente en uso o en fase de desarrollo, un FAQ, y documentación PAM adicional.

Además de estos recursos recomendamos que lea la mayor cantidad de ejemplos de fichero de configuración posible cuando empiece a trabajar con PAM.

Capítulo 8.

Los wrappers TCP y el comando `xinetd`

El control del acceso a los servicios de red puede ser todo un reto. Los firewalls controlan el acceso a una determinada red pero son difíciles de configurar. Para facilitar esta tarea existen los wrappers TCP y el comando `xinetd` controlan el acceso a los servicios basándose en las direcciones IP y en los nombres de las máquinas. Además, estas herramientas también incluyen las funciones de administración y de funcionamiento que son fáciles de configurar.

8.1. Qué son los wrappers TCP

Wrappers TCP están instalados por defecto en la instalación de tipo servidor del sistema operativo Red Hat Linux 8.0 y proporcionan control de acceso a gran variedad de servicios. Muchos servicios modernos de red como por ejemplo SSH, Telnet y FTP usan los *wrappers TCP* , un programa que ha sido diseñado para controlar las peticiones entrantes y los servicios requeridos.

Los wrappers TCP están basados en la idea de que más que permitir la conexión entrante de un cliente directamente con un demonio de servicios de red que se ejecuta como un proceso separado en un sistema de servidores, éstos "capturan" la petición protegiéndola y permitiendo así un mayor control del acceso y de conexión al usuario que esté intentando usar el servicio.

La librería que se encarga de esta funcionalidad es `libwrap.a`, una librería que administra servicios de red como `xinetd`, `sshd` y `portmap` que ya están compilados. También puede compilar otros servicios de red e incluso escribir programas de red con la librería `libwrap.a`. Red Hat Linux proporciona los programas de los wrappers TCP necesarios en el fichero RPM `tcp_wrappers-<version>`.

8.1.1. Ventajas de los wrappers TCP

Cuando alguien intenta acceder a un servicios de red con los wrappers TCP, un programa pequeño de protección da el nombre del servicio requerido y la información de la máquina cliente. Este programa no devuelve ninguna información al cliente y una vez que se cumplen las directivas del control de acceso el programa desaparece evitando así una sobrecarga en la comunicación entre el cliente y el servidor.

Los wrappers TCP ofrecen dos ventajas básicas comparado con las otras técnicas de control de servicios de red:

- *El cliente que se conecta no sabe que se están usando los wrappers TCP.* — Los usuarios legales no notarán ninguna diferencia y los invasores nunca reciben información adicional sobre el motivo por el que las conexiones realizadas fallaron.
- *Los wrappers TCP funcionan independientemente de las aplicaciones que el programa* — Esto permite que muchas aplicaciones puedan compartir un set de ficheros de configuración común facilitando la administración.

8.2. Listas de control de acceso basadas en el nombre de la máquina

El acceso basado en el nombre de la máquina para los servicios que usan wrappers TCP lo controlan dos ficheros: `/etc/hosts.allow` y `/etc/hosts.deny`. Estos ficheros usan un simple formato para controlar el acceso a determinados servicios en un servidor.

Siempre y cuando no se haya especificado ninguna regla en `hosts.allow` y `hosts.deny`, la regla por defecto consiste en permitir a cualquiera acceso a los servicios.

El orden es importante ya que las reglas que se encuentran en `hosts.allow` tienen precedencia con respecto a las especificadas en `hosts.deny`. Aunque una regla deniegue el acceso a un determinado servicio en `hosts.deny`, los clientes que tengan el permiso para acceder al servicio en `hosts.allow` lo mantienen. Todas las reglas de cada uno de los ficheros están colocadas por orden de importancia por lo que hay que respetar dicho orden.

Todos los cambios que se hagan en estos ficheros afectan inmediatamente a los servcios a los que se refieran; no se requiere volver a arrancar los servicios.

8.2.1. Reglas para formatear

Todas las reglas del control de acceso que se encuentran en las líneas `hosts.allow` y `hosts.deny`, y los espacios en blanco o las líneas que empiezan con (#) no se tienen en cuenta. Cada regla tiene que estar en una línea separada.

Las reglas se tienen que formatear de la siguiente manera:

```
<daemon_list>: <client_list>[: <shell_command> ]
```

Cada una de estas opciones se refiere a una parte diversa de la regla:

- `daemon_list` — Es una colección de uno o varios nombres de procesos o de comodines especiales separados por espacios en blanco.
- `client_list` — Uno o varios nombres de máquinas, direcciones de máquina, funciones o comodines separados por espacios en blanco que se usan cuando el nombre de un determinado proceso se adapta a un determinado servicio.
- `shell_command` — Es un componente opcional que indica la realización de algo en el caso de que se use una regla.

Las características son de bastante ayuda cuando se especifican qué grupos de clientes pueden o no tener acceso a un determinado servicio. Así al poner el punto `"."` al comienzo de una cadena, todas las máquinas que se encuentran en esa cadena deben cumplir dicha regla. De tal manera que `.domain.com` engloba tanto a `system1.domain.com` como a `system2.domain.com`. El punto `"."` al final de una cadena tiene el mismo efecto, excepto que el sentido cambia. Esto se usa sobre todo para las direcciones IP ya que una regla relativa a `192.168.0.` se aplica a todo el bloque C de las direcciones IP. Las expresiones de las máscaras de red también se pueden usar como característica para controlar el acceso a un determinado grupo de direcciones IP. También puede usar asteriscos (`*`) o interrogaciones (`?`) para seleccionar grupos enteros de nombres de máquinas o de direcciones IP siempre y cuando no las use en la misma cadena de las otras características.

Si la lista de los nombres de máquinas que tienen acceso a un determinado servicio es muy larga o es difícil de controlar en los ficheros `host.allow` o `hosts.deny`, puede especificar el recorrido completo a un fichero (como `/etc/telnet.hosts.deny`). Este fichero contiene diferentes nombre se máquinas, direcciones de máquinas o características separados por espacios en blanco a los que desea conceder o denegar el acceso a dicho servicio. El método también funciona para compartir las listad de control del acceso entre varios servicios ya que los cambios que se quieran realizar solamente se tienen que hacer en un fichero para que afecten a cada servicio.

Los siguientes comodines se usan en las reglas para el control del acceso en vez de usar determinados nombres de máquinas o grupos de nombres de máquinas:

- `ALL` — Hace corresponder cada cliente a un servicio. Para permitir a una cliente acceso a todos los servicios, utilice `ALL` en la sección de los demonios.
- `LOCAL` — Hace corresponder todos los nombres de máquinas que no contengan un punto `"."`.

- KNOWN — Hace corresponder todas las máquinas cuyos nombres y direcciones se conozcan o en el caso en que se conozcan el usuario.
- UNKNOWN — Hace corresponder todas las máquinas cuyos nombres y direcciones sean desconocidas o en el caso en el que se desconozca el usuario.
- PARANOID — Hace corresponder todas las máquinas cuyo nombre no se corresponda con la dirección.

Atención

Los comodines KNOWN, UNKNOWN y PARANOID tienen que usarse con cuidado porque si se utilizan de una manera incorrecta los usuarios que sí que tengan acceso a un determinado servicio pueden perderlo.

El lenguaje de control del acceso también contiene un operador potente que se llama EXCEPT que permite combinara listas diversas en la misma línea de una regla. Cuando se usa el operador EXCEPT con dos listas, la primera se aplica solo si la entrada procedente de la segunda lista se corresponde con un entidad que cubre la primera lista. El operador EXCEPT se puede usar con las listas de clientes o de demonios. Considere el siguiente ejemplo de hosts.allow:

```
# all domain.com hosts are allowed to connect
# to all services except cracker.domain.com
ALL: .domain.com EXCEPT cracker.domain.com

# 123.123.123.* addresses can use all services except FTP
ALL EXCEPT in.ftpd: 123.123.123.
```

Nota

Normalmente es mejor no usar los operadores EXCEPT si se pueden situar las excepciones a una regla en otro fichero de control del acceso. Esto permite a todos los administradores escanear rápidamente los ficheros apropiados para ver a qué máquinas dar el acceso a un servicio y a cuáles no sin tener que usar varios operadores EXCEPT.

La mejor manera de administrar el control de acceso con los ficheros hosts.allow y hosts.deny es usar los dos ficheros a la vez para así llegar a los resultados deseados.

Los usuarios que desean impedir a otras máquinas el acceso a determinados servicios normalmente ponen ALL: ALL en el fichero hosts.deny. Luego escriben líneas en hosts.allow del tipo:

```
in.telnetd: 10.0.1.24
in.ftpd: 10.0.1. EXCEPT 10.0.1.1
```

Por otro lado, si desea permitir el uso de los servicios de red excepto a algunas máquinas, deje el fichero hosts.allow en blanco y añada cualquier restricción necesaria a hosts.deny, como por ejemplo:

```
in.fingerd: 192.168.0.2
```

Advertencia

Tenga cuidado con el uso de los nombres de máquinas y los nombres de los dominios cuando use los ficheros para el control del acceso especialmente con el fichero `hosts.deny` ya que un invasor puede usar varios trucos para cambiar las reglas de tal manera que le den el acceso. Además, si su sistema permite el acceso seleccionando según el nombre de la máquina y del dominio, toda disfunción del servicio DNS podría impedir el acceso a un determinado servicio incluso a la ususarios que tienen el permiso.

El uso de las direcciones IP cuando sea posible evita muchos problemas a la hora de diseñar reglas de control del acceso, especialmente las que deniegan el acceso.

Para permitir o denegar el acceso a servicios a determinados usuarios aplicando una regla, wrappers TCP también soporta el uso de comandos de la shell. Estos comandos se usan normalmente con las reglas para denegar el acceso que se usan para establecer booby Traps, que generalmente ayudan a mandar información sobre los intentos fallidos a ficheros determinados o correos electrónicos a un administrador. Este es un ejemplo de un "booby trap" situado en el fichero `hosts.deny` que escribe un línea de conexión que contiene la fecha e información del cliente cada vez que una máquina que es encuentra entre los valores 10.0.1.0 y 10.0.1.255 intenta conectarse vía Telnet:

```
in.telnetd: 10.0.1.: (/bin/echo ‘date‘ %c >> /var/log/telnet.log) &
```

Otra característica del uso de comandos de la shell es el soporte de *expansiones*. Expansions proporciona al comando información específica sobre el cliente, el servidor y el proceso. A continuación aparece una lista de las expansiones soportadas

- `%a` — La dirección IP del cliente.
- `%A` — La dirección IP del servidor.
- `%c` — Proporciona información variada sobre el cliente, como el nombre de usuario y el de la máquina o el nombre del usuario y la dirección IP.
- `%d` — El nombre del proceso demonio.
- `%h` — El nombre de la máquina del cliente (o la direccción IP, si el nombre de la máquina no está disponible).
- `%H` — El nombre de la máquina del servidor (o la dirección IP si el nombre de la máquina no está disponible).
- `%n` — El nombre de la máquina del cliente. Si no está disponible aparecerá `unknown`. Si el nombre de la máquina y la dirección de la máquina no se corresponden, aparecerá `paranoid`.
- `%N` — El nombre de la máquina del servidor. Si no est6aacute; disponible aparecerá `unknown`. Si el nombre de la máquina y la dirección de la máquina no coinciden, aparecá `paranoid`.
- `%p` — El ID del proceso demonio.
- `%s` — Información varia del servidor como el proceso demonio y la máquina o la dirección IP del servidor.
- `%u` — El nombre de usuario del cliente. Si no está disponible aparecerá `unknown`.

Para mayor información sobre los comandos de la shell disponibles y otros ejemplos de control del acceso, consulte la página man `hosts_access(5)`.

Nota

Debe de prestar atención cuando use `portmap` con las listas del control del acceso de las máquinas. Solo se podrán usar las direcciones IP o la opción `ALL` para especificar las máquinas a las que dar el acceso o denegarlo ya que no se soportan los nombres de las m´quinas. Además, cambiar las

listas del control del acceso de las máquinas relativas al comando portmap no tienen un efectivo inmediato.

Debido a que servicios tan usados como NIS y NFS dependen del comando portmap tenga en cuenta estas limitaciones antes de usar los ficheros hosts.allow y hosts.deny para controlar el acceso.

8.3. Control del acceso con el comando xinetd

Los beneficios de que ofrecen los wrappers TCP son todavía mayores cuando se usa la librería libwrap.a junto con el comando xinetd, un *super-demonio* que ofrece acceso adicional, conexión, vinculación, redirección y control del uso de los recursos.

El sistema operativo Red Hat Linux configura una variedad de servicios de red famosos que se usan con el comando xinetd como FTP, IMAP, POPy telnet. Cuando se accede a cualquiera de estos servicios a través de sus números de puerta en el fichero /etc/services, el demonio xinetd es el encargado de llevar a cabo esta petición. Antes de que el usuario que tiene el acceso lleve a cabo el servicio requerido, el comando xinetd se asegura que la imformación de la máquina cliente cumpla las reglas del control del acceso, el número de instancias del servicio que se encuentre en un subproceso y todas las reglas específicas para dicho servicio o que se cumplan todos los servicios xinetd. Una vez que se ha obtenido el servicio deseado, el comando xinetd se apaga hasta que se haga otra nueva petición del servicio que administra.

8.3.1. Ficheros de configuración del comando xinetd

El servicio xinetd lo controla el fichero /etc/xinetd.conf así como otros ficheros específicos que se encuentran en el directorio /etc/xinetd.d/

8.3.1.1. /etc/xinetd.conf

El fichero xinetd.conf es el padre de todos los ficheros de configuración del comando xinetd ya que todos los ficheros de servicios determinados también se sintetizan cada vez que se activa el comando xinetd. Por defecto, el fichero xinetd.conf contiene pautas de configuración básicas que se aplican a cada servicio. A continuación aparece un ejemplo de un xinetd.conf típico:

```
defaults
{
 instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success  = HOST PID
        log_on_failure  = HOST
        cps                     = 25 30
}

includedir /etc/xinetd.d
```

Estas líneas controlan varios aspectos de xinetd:

- instances — Establece el número máximo de peticiones que un determinado servicio puede administrar a la vez.
- log_type — Dice al comando xinetd que use el log authpriv que se encuentra especificado en el fichero /etc/syslog.conf y establece el fichero /var/log/secure por defecto en vez de

usar otro fichero específico. Si se usa la opción `FILE /var/log/xinetdlog` el comando `xinetd` se colocaría en el fichero `/var/log/xinetdlog`.

- `log_on_success` — Permite al comando `xinetd` conocer a qué se debe conectar si la conexión tiene éxito. Por defecto, la dirección IP de la máquina remota y la ID del proceso del servidor que procesa la petición están grabadas.
- `log_on_failure` — Dice al comando `xinetd` a qué se tiene que conectar si la conexión no tiene éxito.
- `cps` — Le dice al comando `xinetd` que no permita más de 25 conexiones por segundo a un servicio dado. Si se alcanza este límite, el servicio se retira durante 30 segundos.

Nota

Ambas configuraciones `log_on_success` y `log_on_failure` en `/etc/xinetd.conf` se modifican a menudo por cada servicio, lo que significa que conexiones logradas y fallidas normalmente cargarán más información de la que se indica en `/etc/xinetd.conf`.

Existen varias opciones de conexión disponibles en el fichero `/etc/xinetd.conf` y en los ficheros de configuración de los servicios especiíficos `xinetd`:

- `ATTEMPT` — Indica que se intentó realizar una conexión pero que ésta falló (`log_on_failure`)
- `DURATION` — Indica el tiempo que usa un servicio un sistema remoto (`log_on_success`)
- `EXIT` — Indica el estado de salida o la señal de témino del servicio. (`log_on_success`)
- `HOST` — Indica la dirección IP de la máquina remota.(`log_on_failure` y `log_on_success`)
- `PID` — Indica el Id del proceso del servidor que recibe la petición.(`log_on_success`)
- `RECORD` — Graba información sobre el sistema remoto en el caso de que no se pueda iniciar el servicio. Esta opción la usan solo determinados tipos de servicios como `login` y `finger`. (`log_on_failure`)
- `USERID` — Indica el usuario remoto que está usando el método definido en RFC 1413 para todos los servicios de multi procesos. (`log_on_failure` y `log_on_success`)

Existen otras opciones disponibles para el fichero `/etc/xinetd.conf` como por ejemplo `per_source` que limita el número máximo de conexiones de una dirección IP específica a un servidor determinado. Para más información consulte las páginas de manual de `xinetd`

8.3.1.2. Ficheros en el directorio `/etc/xinetd.d`

Los ficheros que se encuentran en el directorio `/etc/xinetd.d` se leen cada vez que se inicia el comando `xinetd` debido al argumento `includedir /etc/xinetd.d` que se encuentra al final del fichero `/etc/xinetd.conf`. Estos ficheros con nombres como `finger`, `ipop3` y `rlogin` se refieren a los diversos servicios que controla el comando `xinetd`.

Los ficheros del directorio `/etc/xinetd.d` usan los mismos convenios que `/etc/xinetd.conf`. La razón principal por la que se encuentran en ficheros separados, cada uno para un servicio, es que así se pueden añadir y eliminar servicios del dominio del comando `xinetd` sin afectar a otros servicios.

Para hacerse una idea de la estructura de estos ficheros, considere el fichero `wu-ftp`:

```
service ftp
{
        socket_type             = stream
        wait                    = no
```

```
        user                    = root
        server                  = /usr/sbin/in.ftpd
        server_args             = -l -a
        log_on_success          += DURATION USERID
        log_on_failure          += USERID
        nice                    = 10
        disable                 = yes
}
```

La primera línea define el nombre del servicio. Las líneas que se encuentran entre paréntesis contienen las diferentes características que definen cómo se debe usar el servicio y cómo se inicia. El fichero `wu-ftp` afirma que el servicio FTP usa la opción `stream` en el tipo de enchufe (mejor que la opción `dgram`), el fichero binario ejecutable, los argumentos que se pasan al binario, la información que hay que añadir a las características del directorio `/etc/xinetd.conf`, la prioridad con la que hay que ejecutar el servicio y otros datos.

El uso del comando `xinetd` con un servicio también sirve como nivel básico de protección contra el ataque del DoS. La opción `max_load` toma un valor de un punto flotante para configurar el punto de acción del uso CPU cuando no se acepten más conexiones a un servicio evitando así que se sobrecargue el sistema. La opción `cps` acepta un valor de integración para establecer el límite de las conexiones disponibles por segundo. La configuración de este valor debe de tener un valor bajo como por ejemplo `3` por que así se evita que los invasores del sistema puedan inundar el sistema con peticiones simultáneas de un servicio particular.

8.3.1.3. Control del acceso con el comando xinetd

Los usuarios de los servicios `xinetd` pueden elegir los ficheros de control de acceso con los wrappers TCP (`/etc/hosts.allow` y `/etc/hosts.deny`) que ofrecen el control del acceso vía los ficheros de configuración `xinetd` o la mezcla de ambos. Para mayor información sobre el control del acceso con los wrappers TCP consulte la Sección 8.2 en la que encontrará todo lo referente al comando `xinetd`.

Nota

A diferencia de los ficheros de control de acceso con los wrappers TCP, todo cambio que se realice en los ficheros de configuración `xinetd` requiere el reinicio del servicio `xinetd` así como el reinicio de todos los servicios para que éstos tengan efecto.

El comando `xinetd` para el control del acceso disponible en los diversos ficheros de configuración es distinto para cada uno de los métodos que usan los wrappers TCP. Mientras que los wrappers TCP sitúan toda la configuración del acceso en dos ficheros,`/etc/hosts.allow` y `/etc/hosts.deny`, cada uno de los ficheros del servicio que se encuentran en el directorio `/etc/xinetd.d` pueden contener las reglas de control del acceso que se basan en las máquinas que están autorizadas para usar dicho servicio.

Las siguientes opciones están soportadas en los ficheros `xinetd` para controlar el acceso de las máquinas:

- `only_from` — Permite que las máquinas específicas usen el servicio.
- `no_access` — Impide que estas máquinas usen el servicio.
- `access_times` — Especifica el intervalo de uso de un determinado servicio el cual de encuentra en un formato `HH:MM-HH:MM` que usa notas las 24 horas del día.

Las opciones only_from y no_access pueden usar una lista de direcciones IP o nombres de las máquinas o pueden especificar también toda la red. Como ocurre con los wrappers TCP, la combinación del comando xinetd para el control del acceso con una configuración de conexión apropiada para dicho servicio no solo le permite impedir la petición sino también grabar cada intento de acceso.

Por ejemplo, el siguiente fichero /etc/xinetd.d/telnet se puede usar para impedir el acceso a telnet a un sistema con un grupo de red particular y restringir el intervalo de conexión incluso a los usuarios autorizados:

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        no_access       = 10.0.1.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

En este ejemplo, cuando un sistema de la subred 10.0.1.0/24 como por ejemplo la 10.0.1.2, intenta conectarse a telnet en la máquina, recibe el mensaje Connection closed by foreign host.(Máquina extraña cierra la conexión) Además, el intento de conexión aparece en /var/log/secure:

```
May 15 17:35:47 boo xinetd[16188]: START: telnet pid=16191 from=10.0.1.2
May 15 17:38:49 boo xinetd[16252]: START: telnet pid=16256 from=10.0.1.2
May 15 17:38:49 boo xinetd[16256]: FAIL: telnet address from=10.0.1.2
May 15 17:38:49 booxinetd[16252]: EXIT: telnet status=0 pid=16256
```

8.3.1.4. Vinculación y desvío del puerto

Los ficheros de configuración de servicios para el comando xinetd también soportan la vinculación del servicio a una dirección IP y el desvío de las peticiones entrantes para dicho servicio a otra dirección IP, nombre de la máquina o puerto.

La vinculación es controlada con la opción bind que se encuentra en los ficheros de configuración, y une específicamente el servicio a una dirección IP que se encuentre en uso en el sistema. Al usarla, la opción bind permite solo las peticiones que usan esa dirección IP para acceder al servicio. Cada servicio se une a diferentes interfaces de red basándose en sus necesidades. Esto es útil sobre todo para los sistemas con múltiples adaptadores de red que usan varias direcciones IP. Por ejemplo, puede configurar telnet de modo que solo escuche a la interfaz conectada a una red privada, y no a la interfaz conectada a Internet.

La opción redirect acepta la dirección IP o el nombre de la máquina seguido del número de puerto. Dice al servicio que desvíe todas las peticiones para dicho servicio a una localización y número de puerto específicos. Esta característica se usa para establecer otro número de puerto en el mismo sistema, desviar la petición a otra dirección IP en la misma máquina, cambiar la petición a otro sistema y puerto completamente diferentes o con la combinación de cualquiera de estas opciones. De esta manera, un usuario que está conectado a un determinado servicio en un sistema puede desviar su petición a otro sistema sin provocar ninguna disfunción.

El demonio xinetd lleva a cabo este desvío lanzando un proceso que mantenga la conexión entre la máquina cliente que está mandando la petición y la máquina que está dando en ese momento el servicio, transfiriendo los datos de un sistema a otro.

El mayor beneficio de estas dos opciones se obtiene cuando se usan juntas. Vinculando un servicio a una dirección IP determinada en un sistema y luego desviando las peticiones de dicho servicio a una segunda máquina que solo puede ver la primera máquina, se puede usar un sistema interno que ofrezca servicios para una red completamente diversa. Alternativamente, estas opciones se pueden usar para limitar la exposición de un servicio determinado a una dirección IP determinada así como desviar todas las peticiones de ese servicio a otra máquina configurada específicamente para ese objetivo.

Por ejemplo, considere un sistema que se usa como firewall con la característica siguiente para el servicio FTP:

```
service ftp
{
        socket_type  = stream
        wait   = no
        user   = root
        server   = /usr/sbin/in.ftpd
        server_args  = -l -a
        log_on_success  += DURATION USERID
        log_on_failure  += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 21
}
```

Las opciones `bind` y `redirect` en este fichero aseguran que el servicio FTP en la máquina esté vinculado a la dirección IP externa (123.123.123.123), la que se encarga de Internet`/etc/xinetd.d`. Además, todas las peticiones del servicio FTP que se han mandado a la dirección 123.123.123.123 se desvín a través de un segundo adaptador de red a una dirección IP (10.0.1.13) a la que solo tienen acceso el firewall y los sistemas internos. El firewall manda luego la comunicación a los dos sistemas y el sistema que se está conectando piensa que está conectado a la dirección 123.123.123.123 mientras que, de hecho, está conectado a otra máquina.

Esta característica es útil para los usuarios con conexiones de banda amplia y con una única dirección IP. Cuando se usa la Traducción de las direcciones de la red, la NAT, los sistemas se ocultan en la máquina de puerta de enlace que usa las direcciones IP internas y no están disponibles en el sistema de puerta de enlace externo. Sin embargo, cuando determinados servicios que controla el comando `xinetd` se configuran con las opciones `bind` y `redirect`, la m´quina de puerta de enlace actuar como proxy entre los sistemas externos. Además, las opciones para el control del acceso `xinetd` y para la conexión también se encuentran disponibles para una protección adicional como por ejemplo limitar el número de conexiones simultáneas para el servicio que ha sido desviado.

8.4. Recursos adicionales

Puede obtener más información sobre los wrappers TCP y el comando `xinetd` en su sistema y en la web.

8.4.1. Documentación instalada

La documentación de su sistema es una buena fuente de información sobre los wrappers TCP, el comando `xinetd` y las opciones de configuración del control del acceso.

- `/usr/share/doc/tcp_wrappers-`<*version*> — Contiene un fichero `README` que trata el funcionamiento de los wrappers TCP y de los riesgos que pueden correr diversos nombres de máquinas y de direcciones de máquinas.

- /usr/share/doc/xinetd-<*version*> — Incluye un fichero README que trata los aspectos del control de acceso y un fichero sample.conf con varias ideas para modificar las configuraciones del servicio /etc/xinetd.d.
- Para mayor información sobre las reglas de cómo crear wrappers TCP, consulte las páginas man hosts_access (sección 5) y hosts_options.
- Las páginas man xinetd y xinetd.conf contienen información adicional para la creación de ficheros de configuración xinetd y una descripción del funcionamiento del comando xinetd.

8.4.2. Sitios web útiles

- http://www.xinetd.org — xinetd, contiene ejemplos de ficheros de configuración, una lista completa de características y FAQs informativas.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — Trata las distintas maneras de usar los ficheros de configuración xinetd para alcanzar determinados objetivos de seguridad.

Capítulo 9.

Protocolo SSH

SSH™ permite a los usuarios registrarse en sistemas de host remotamente. A diferencia de `rlogin` o `telnet` SSH encripta la sesión de registro imposibilitando que alguien pueda obtener una contraseña de texto.

SSH está diseñado para reemplazar los métodos comunes para registrarse remotamente en otro sistema a través de la shell de comando. El programa `scp` reemplaza otros programas diseñados para copiar ficheros entre hosts como por ejemplo `ftp` o `rcp`. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, las evita siempre que sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas hará disminuir los riesgos de seguridad para ambos sistemas y el sistema remoto.

9.1. Introducción

SSH (o Secure *SH*ell) es un protocolo para crear conexiones seguras entre dos sistemas. Usando SSH, la máquina del cliente inicia una conexión con una máquina del servidor.

SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor durante sesiones ulteriores.
- El cliente puede transmitir su información de autenticación al servidor, como el nombre de usuario y la contraseña, en formato cifrado.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de encriptación fuerte, lo cual los hacen extremamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de usar X11 [1] aplicaciones lanzadas desde el intérprete de comandos de la shell. Esta técnica proporciona una interfaz gráfica segura (llamada *reenvío por X11*), proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede converrirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada *reenvío por puerto*, como por ejemplo POP, incrementando la seguridad del sistema en general y de la seguridad de los datos.

Red Hat Linux 8.0 contiene el paquete general de OpenSSH (`openssh`), el servidor de OpenSSH (`openssh-server`) y los paquetes de clientes (`openssh-clients`). Consulte el capítulo titulado *OpenSSH* en el *Manual oficial de personalización de Red Hat Linux* para obtener instrucciones sobre la instalación y el desarrollo de OpenSSH. Observe que los paquetes OpenSSH requieren el paquete OpenSSL (`openssl`). OpenSSL instala varias librerías criptográficas importantes que ayudan a OpenSSH a proporcionar comunicaciones encriptadas.

Una gran cantidad de programas de cliente y servidor puede usar el protocolo SSH, incluyendo muchas aplicaciones open source a disposición gratuita. Hay varias versiones de cliente diferentes de SSH a disposición para casi todos los sistemas operativos más importantes en uso actualmente. Aún si los usuarios que se conectan a su sistema no ejecutan Red Hat Linux, de cualquier manera pueden encontrar y usar un cliente de SSH nativo para su sistema operativo.

1. X11 se refiere al sistema de visión por ventanas X11R6, tradicionalmente llamado X. Red Hat Linux contiene **XFree86**, un sistema X Window open-source muy conocido, que se basa en X11R6.

9.1.1. ¿Porqué usar SSH?

Los usuarios ajenos a su ordenador poseen diversas herramientas para interceptar y dirigir el tráfico de la red de manera que tengan accesos a su sistema. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

- *Intercepción de la comunicación entre dos sistemas* — bajo esta hipótesis, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información, o puede modificar la información y luego enviarla al recipiente al cual estaba destinada. Esto se produce usando la utilidad sniffer.
- *Personificación de un determinado host* — con esta estrategia, un sistema interceptor finge ser el recipiente a quien está destinado un mensaje. Si funciona la estrategia, el cliente no se da cuenta del engaño y continúa la comunicación con el interceptor como si su mensaje hubiese llegado a su destino satisfactoriamente. Esto se produce con técnnicas como el envenenamiento del DNS. [2] [3].

Ambas técnicas causan que se intercepte información, posiblemente con propósitos hostiles. El resultado puede ser catastrófico.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar ficheros, estas amenazas a la seguridad se pueden disminuir notablemente. La firma digital de un servidor proporciona la verificación para su identidad. No es posible utilizar la comunicación entera entre los sistemas si ha sido interceptada, porque cada uno de los paquetes está cifrado. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

9.2. Secuencia de eventos de una conexión SSH

Una cierta serie de eventos ayuda a proteger la integridad de una comunicación SSH entre dos hosts.

Primero, se crea una *capa de transporte* segura para que el cliente sepa que está efectivamente comunicando con el servidor correcto. Luego se cifra la comunicación entre el cliente y el servidor por medio de un código simétrico.

Después, con la conexión segura al servidor en su lugar, el cliente se autentica ante el servidor sin preocuparse de que la información de autenticación pudiese exponerse a peligro.

Por último, con el cliente autenticado ante el servidor, se pueden usar varios servicios diferentes con seguridad a través de la conexión, como una sesión shell interactiva, aplicaciones X11 y túneles TCP/IP.

9.3. Capas de seguridad SSH

El protocolo SSH permite que cualquier programa de cliente y servidor construido según los planes detallados del protocolo comuniquen con seguridad y se usen de manera intercambiable.

Actualmente existen dos variedades diferentes de SSH. La versión 1 de SSH contiene varios algoritmos de encriptación patentados (sin embargo varios de estas patentes han caducado) y un agujero de seguridad que potencialmente permitiría que datos se inserten en el flujo de datos. Se recomienda el uso de servidores y clientes compatibles con la versión 2 de SSH, si es posible.

2. El envenenamiento del DNS ocurre cuando un intruso entra en el servidor de los DNS, apuntando el sistema hacia hosts intencionalmente duplicados o spoofing del IP.
3. IP spoofing ocurre cuando un intruso manda paquetes de red que parecen provenir de hosts de confianza de la red.

Las versiones de protocolo SSH 1 y 2 añaden capas de seguridad, cada una añade su propio tipo de protección.

9.3.1. Capa de transporte

El papel principal de la capa de transporte es el de facilitar una comunicación segura entre dos hosts a la hora de y después de la autenticación. Normalmente ejecutado a través de TCP/IP, la capa de transporte logra hacer esto ocupándose de la encriptación y descifrado de datos, verificando que el servidor sea la máquina correcta para la autenticación, y proporcionando protección a la integridad de los paquetes de datos al momento de ser enviados y recibidos. Además, la capa de transporte también puede proveer la compresión de los datos, acelerando así la transmisión de la información.

Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de transporte correctamente. Durante el intercambio se producen los siguientes pasos:

- Intercambio de claves
- El algoritmo de la clave pública que hay que usar
- El algoritmo de la encriptación simétrica que hay que usar
- El algoritmo de la autenticación de mensajes que hay que usar
- El algoritmo de hash que hay que usar

El servidor se identifica ante el cliente con una *clave de host* durante el intercambio de claves. Obviamente si este cliente nunca había comunicado antes con este determinado servidor, la clave del servidor le resultará desconocida al cliente. OpenSSH evita este problema permitiendo que el cliente acepte la clave de host del servidor la primera vez que se lleva a cabo una conexión SSH. Luego la clave de host del servidor se puede verificar con la versión guardada en el cliente en las siguientes conexiones, proporcionando la confianza que el cliente está realmente comunicando con el servidor deseado.

Advertencia

Un agresor podría enmascararse como servidor SSH durante el contacto inicial ya que el sistema local no conoce la diferencia entre el servidor en cuestión y el falso configurado por un agresor. Pare evitar que esto ocurra debería verificar la integridad del nuevo servidor SSH contactando con el adiministrador del servidor antes de conectarse por primera vez.

SSH fue ideado para funcionar con casi cualquier tipo de algoritmo de clave pública o formato de codificación. Después de que el intercambio de claves inicial crea dos valores (un valor de hash usado para intercambios y un valor de secreto compartido), los dos sistemas empiezan inmediatamente a calcular claves y algoritmos nuevos para proteger la autenticación y los datos que se enviarán a través de la conexión en el futuro.

Después que una cierta cantidad de datos haya sido transmitida con un determinado algoritmo y clave (la cantidad exacta depende de la ejecución de SSH), ocurre otro intercambio de claves, el cual genera otro conjunto de valores de hash y un valor de secreto compartido. De esta manera aunque un agresor lograse determinar los valores de hash y de secreto compartido, deberá repetir todo el procedimiento después de un intercambio de claves nuevo para poder continuar a supervisar la comunicación.

9.3.2. Autenticación

Cuando la capa de transporte haya construido un túnel seguro para transmitir información entre los dos sistemas, el servidor le dirá al cliente de los diferentes métodos de autenticación soportados, como el uso de firmas privadas codificadas con claves o la inserción de una contraseña. El cliente entonces intentará autenticarse ante el servidor mediante el uso de cualquiera de los métodos soportados.

Ya que los servidores se pueden configurar para que concedan varios tipos de autenticación, este método proporciona a cada parte un control óptimo. Luego el servidor podrá decidir qué métodos de encriptación soportará basado en su pauta de seguridad, y el cliente puede elegir el orden en que intentará utilizar los métodos de autenticación entre las opciones a disposición. Gracias a la naturaleza segura de la capa de transporte de SSH, hasta métodos de autenticación que parecen inseguros, como la autenticación basada en el host, son en realidad seguros.

La mayoría de los usuarios que requieren de una shell segura se autenticarán por medio de una contraseña. Ya qeu la contraseña está encriptada en el proceso de envío, se puede enviar fácilmente a través de la red.

9.3.3. Conexión

Después de una autenticación exitosa sobre una capa de transporte SSH, se abren *canales* múltiples por medio de la multiplexión[4] la conexión individual entre dos sistemas. Cada canal se ocupa de la comunicación para sesiones entre terminales diferentes, el reenvío de información por X11 o cualquier servicio aparte que intente usar la conexión SSH.

Ya sea los clientes como los servidores pueden crear un canal nuevo, con cada canal asignado un número diferente en cada orilla. Cuando una parte intenta abrir un canal nuevo, el número para el canal de esa parte se envía junto con la petición. Esta información se almacena por la otra parte y se usa para dirigir un determinado tipo de comunicación de servicio a ese canal. Esto se lleva a cabo para que diferentes tipos de sesiones no se afecten los unos por los otros y que los canales puedan cerrarse sin interrumpir la conexión SSH principal entre los dos sistemas.

Los canales también soportan el control de flujo, el cual les permite enviar y recibir datos ordenadamente. De esta manera, los datos no se envían a través del canal sino hasta que el host haya recibido un mensaje avisando que el canal puede recibirlos.

Los canales son especialmente útiles con el reenvío por X11 y el reenvío por puerto TCP/IP con SSH. Se pueden configurar canales aparte en modo diferente, tal vez para usar un tamaño de paquete máximo diferente o para transferir un determinado tipo de datos. Esto permite que SSH sea flexible en su modo de encargarse de los diferentes tipos de conexiones remotas, como el acceso telefónico en redes públicas o enlaces LAN de alta velocidad, sin tener que cambiar la infraestructura básica del protocolo.

9.4. Ficheros de configuración OpenSSH

OpenSSH tiene dos conjuntos diferentes de ficheros de configuración, uno para los programas del cliente (`ssh`, `scp`, y `sftp`) y el otro para los servicios del servidor (`sshd`), ubicados en dos sitios diferentes.

La información de configuración SSH para todo el sistema está almacenada en el directorio `/etc/ssh`:

4. Una conexión multiplexada consiste en varias señales enviadas simultáneamente por un medio compartido. Con SSH, se envían varios canales en una conexión en común segura.

- `moduli` — Contiene grupos Diffie-Hellman usados para el intercambio de la clave Diffie-Hellman que es imprescindible para la construcción de una capa de transporte seguro. Cuando se intercambian las claves al inicio de una sesión SSH, se crea un valor secreto y compartido que no puede ser determinado por ambas partes a la misma vez. Este valor se usa para proporcionar la autentificación del host.
- `ssh_config` — fichero de configuración del cliente SSH por defecto que se sobreescribe si éste está persente el el directorio principal del usuario (`~/.ssh/config`).
- `sshd_config` — el fichero de configuración para `sshd`.
- `ssh_host_dsa_key` — la clave privada DSA usada por `sshd`.
- `ssh_host_dsa_key.pub` — la clave pública DSA usada por `sshd`.
- `ssh_host_key` — la clave privada RSA usada por `sshd` para la versión 1 del protocolo SSH.
- `ssh_host_key.pub` — la clave pública RSA usada por `sshd` para la versión 1 del protocolo SSH.
- `ssh_host_rsa_key` — la clave privada RSA usada por `sshd` para la versión 2 del protocolo SSH.
- `ssh_host_rsa_key.pub` — la clave pública RSA usada por `sshd` para la versión 2 del protocolo SSH.

La información para la configuración SSH específica para el usuario está almacenada en el directorio principal `~/.ssh/`:

- `authorized_keys` — el fichero que contiene una lista de claves públicas "autorizadas". Si un usuario que se conecta puede comprobar que conoce la clave privada que corresponde a cualquiera de las claves públicas, entonces será autenticada. Note que esto es sólo un método de autenticación opcional.
- `id_dsa` — contiene la identidad de autenticación DSA del usuario.
- `id_dsa.pub` — la clave pública DSA del usuario.
- `id_rsa` — La clave pública RSA usada por `sshd` para la versión 2 del protocolo SSH.
- `identity` — La clave privada RSA usada por `sshd` para la versión 1 del protocolo SSH.
- `known_hosts` — Este fichero contiene las claves de host DSA de los servidores SSH a los que se accede mediante el usuario. Este fichero es muy importante para asegurse de que el cliente SHH está conectado al servidor SSH correcto. Si se ha cambiado una clave de host y no está seguro del porqué, debería contactar con el administrador del sistema del servidor SSH para asegurarse de que el servidor no está comprometido. Si las claves de host del servidor están alteradas legitimamente debido a una reinstalación de Red Hat Linux, la próxima vez que se registre en aquel servidor se le notificará que la clave del host almacenada en el fichero `known_hosts` no coincide. Para conectarse al servidor, el usuario debe abrir el fichero `known_hosts` en un editor de textos y borrar la clave para ese host. Esto permite que el cliente SSH cree una nueva clave de ho! st.

Consulte las páginas de manual `ssh` y `sshd` para obtener información acerca de las directivas disponibles en los ficheros de configuración SSH.

9.5. Más que una shell segura

Una interfaz de línea de comandos segura es sólo el inicio de las muchas maneras de usar SSH. Dada una cantidad apropiada de ancho de banda, las sesiones X11 se pueden dirigir por un canal SSH. O se pueden asignar conexiones de puerto entre sistemas que previamente eran inseguras a canales SSH específicos usando el reenvío por TCP/IP.

9.5.1. Reenvío por X11

Abrir una sesión X11 a través de una conexión SSH establecida es tan fácil como ejecutar un programa X mientras se está ya ejecutando un cliente X en su host. Cuando un programa X se ejecuta desde un intérprete de comandos de shell segura, el cliente y el servidor SSH crean un nuevo canal seguro dentro de la conexión SSH actual, y los datos del programa X se envían a través de ese canal a la máquina de cliente como si usted estuviese conectado al servidor X por medio de una terminal local.

Como podrá imaginar, el reenvío por X11 puede ser muy útil. Por ejemplo, se puede usar el reenvío por X11 para crear una sesión segura e interactiva con el GUI `up2date` en el servidor para actualizar paquetes en modo selectivo. Para hacer esto simplemente hay que conectarse al servidor mediante `ssh` y teclear:

```
up2date &
```

Se le pedirá proporcionar la contraseña de root para el servidor. Luego aparecerá el **Red Hat Update Agent** y usted podrá actualizar sus paquetes en el servidor como si estuviese sentado delante de la máquina.

9.5.2. Reenvío del puerto

Con SSH puede asegurar los protocolos TCP/IP a través del reenvío de puertos. Cuando use esta técnica, el servidor SSH se convierte en un conducto encriptado para el cliente SSH.

El reenvío de puertos funciona mediante el mapeado de un puerto local en el cliente para un puerto remoto del servidor. SSH le permite mapear cualquier puerto desde el servidroa cualquier puerto en el cliente; los números de puerto no necesitan coincidir para poder funcionar.

Para crear un canal de reenvío de puerto TCP/IP que escucha conexiones del host local, utilice el siguiente comando:

```
ssh -L local-port:remote-hostname:remote-port username@hostname
```

Nota

La configuración del reenvío de un puerto para que escuche puertos bajo 1024 requiere acceso de root.

Si desea comprobar su correo en el servidor llamado mail.domain.com mediante el uso de POP a través de una conexión encriptada, puede usar el siguiente comando:

```
ssh -L 1100:mail.domain.com:110 mail.domain.com
```

Una vez que el canal de reenvío de puerto está entre las dos máquinas, puede direccionar su cliente de correo POP para usar el puerto 1100 en su host local para comprobar el nuevo correo. Cualquier petición enviada la puerto 1100 en su sistema será dirigida seguramente al sevidor mail.domain.com.

Si mail.domain.com no está ejecutando un demonio del servidor SSH, pero puede registrarse a través de SSH a una máquina el la misma red, puede usar SSH para asegurar la parte de la conexión POP. No obstante, se necesita un comando diferente:

```
ssh -L 1100:mail.domain.com:110 other.domain.com
```

En este ejemplo, se está reenviando su petición POP desde el puerto 1100 en su máquina a través de una conexión SSH en el puerto 22 para other.domain.com.. `other.domain.com` conecta el puerto

110 en `mail.domain.com` para permitirle que compruebe este nuevo correo. Mediante el uso de este técnica, sólo es segura la conexión entre su sistema y `other.domain.com`.

El reenvío del puerto se puede usar para obtener información segura a través de los firewalls de red. Si el firewall está configurado para permitir el tráfico SSh a través del puerto estándar (22) pero bloquea el acceso a través de otros puertos, es posible todavía una conexión entre dos hosts usando los puertos bloqueados al redireccionar la comunicación sobre una conexión SSH establecida.

Nota

Mediante el uso del reenvío de puerto para reenviar conexiones de este modo permiten al usuario en el sistema cliente conectarse al servicio al que se están reenviando las conexiones. Si el sistema de cliente se convierte en un sistema comprometido, el agresor tendrá acceso a los servicios reenviados.

Los administradores del sistema preocupados por el reenvío del puerto pueden deshabilitar esta funcionalidad en el servidro especificando un parámetro `No` para la línea AllowTcpForwarding en `/etc/ssh/sshd_config` y reiniciar el servicio `sshd`.

9.6. Requisitos de SSH para conexiones remotas

Para que SSH sea realmente eficaz para proteger sus conexiones de red, deberá dejar de usar protocolos de conexión inseguros, como por ejemplo `telnet` y `rsh`. De otra manera, la contraseña de un usuario podría ser protegida un día si se usa `ssh` y luego ser capturada al día siguiente cuando inicia una sesión por medio de `telnet`.

Para deshabilitar los métodos de conexiones inseguras para su sistema, utilice el programa de línea de comandos `chkconfig`, el programa compatible ncurses `ntsysv`, o la aplicación gráfica **serviceconf**. Todas estas herramientas requieren el acceso a root.

Algunos servicios a deshabilitar incluyen:

- `telnet`
- `rsh`
- `ftp`
- `rlogin`
- `wu-ftpd`
- `vsftpd`

Para más información sobre los niveles de ejecución y servicios de configuración con `chkconfig`, `ntsysv` y **Herramienta de configuración de servicios**, remítase al capítulo titulado *Control del acceso a servicios* en el *Manual oficial de personalización de Red Hat Linux.*

Capítulo 10.

Kerberos

Kerberos es un protocolo de seguridad creado por MIT que usa una criptografía basada en claves secretas — evitando así tener que enviar contraseñas por medio de la red. Al autentificar por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

10.1. ¿Por qué usar Kerberos?

La mayoría de las redes usan esquemas de autenticación basados en contraseñas. Cuando un usuario necesita una autenticación en un servidor de red, debe proporcionar un nombre de usuario y una contraseña para cada servicio que requiere autenticación. La información se envía a través de la red y el servidor verifica su identidad usando dicha información.

La transmisión de información de autenticación para es en texto plano para muchos servicios. Cualquier intruso del sistema con acceso a la red y un analizador de paquetes puede interceptar cualquier contraseña enviada de este modo.

El primer objetivo de Kerberos es el de eliminar la transmisión a través de la red de información de autenticación. Un uso correcto de Kerberos erradica la amenaza de analizadores de paquetes que intercepten contraseñas en su red.

10.2. ¿Por qué no usar Kerberos?

Kerberos elimina una amenaza de seguridad común. ¿Por qué no se usa en todas las redes? Por varias razones, kerberos puede ser difícil de implementar:

- No existe ninguna solución rápida para migrar contraseñas de usuarios desde una base de datos de contraseñas UNIX (tales como `/etc/passwd` o `/etc/shadow`) a una base de datos de contrseñas Kerberos. La migración es técnicamente posible, pero es un tema que se escapa del dominio de este capítulo. Para más información, consulte la pregunta 2.23 en las FAQ de Kerberos en la siguiente URL http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html.
- Kerberos es solo parcialmente compatible con los Pluggable Authentication Modules (PAM) usados por la mayoría de los servidores en Red Hat Linux. Para más información vea la Sección 10.5.
- Para una aplicación use Kerberos, el código debe ser modificado para hacer las llamadas apropiadas a las librerías de Kerberos. Para algunas aplicaciones, esto puede suponer un esfuerzo excesivo de programación. Para otras aplicaciones, los cambios se deben realizar en el protocolo usado entre el servidor de red y sus clientes; de nuevo, esto puede suponer una programación excesiva. Además, resultará imposible hacer que ciertas aplicaciones de código fuente cerrado funcionen con Kerberos.
- Kerberos presupone que usted está utilizando hosts fiables en una red no fiable. Su primer objetivo es el de prevenir que las contraseñas de texto plano sean enviadas a través de la red. Sin embargo, si cualquier otro a parte del usuario adecuado tiene acceso físico a cualquiera de los hosts, especialmente el que emite tickets usados para la autenticación, todo sistema de autenticación de Kerberos corre el riesgo de transigir.
- Finalmente, si decide usar Kerberos en su red, debe darse cuenta de que es una elección de todo o nada. Si *alguno* de los servicios que transmite las contraseñas de texto sin retocar permanece en uso, las contraseñas pueden todavía estar comprometidas y su red no se beneficiará del uso de Kerberos. Para asegurar su red con Kerberos, debe *kerberizar* (hacer trabajar con Kerberos) *todas*

las aplicaciones que mandan las contraseñas en texto plano o parar el uso de esta aplicaciones en la red.

10.3. Terminología Kerberos

Como algunos otros sistemas, Kerberos tiene su propia terminología. Aquí hay una lista de términos que necesitará para estar familiarizado:

texto cifrado

datos encriptados

texto plano

Datos no encriptados, legibles.

cliente

Una entidad de la red (un usuario, un host o una aplicación) que toma un ticket de Kerberos.

caché credencial o archivo de tickets

Un fichero que contiene las claves para encriptar las comunicaciones entre el usurario y varios servicios de red. Kerberos 5 proporciona un framework para usar otros tipos de caché (como la memoria compartida), pero los archivos están mejor soportados.

hash encriptado

Un hash de un sentido usado para autentificar usuarios. Aunque es más seguro que el texto plano, es bastante fácil desencriptarlo para un cracker con experiencia.

clave

Dato usado cuando encriptamos o desencriptamos otros datos. Los datos encriptados no pueden ser desencriptados sin la clave apropiada.

Centro de distribución de claves (KDC)

Un servicio que emite tickets Kerberos, que habitualmente se ejecutan en el mismo host como un Ticket Granting Server.

dominio

Red que usa Kerberos, compuesto de uno o varios servidores (también conocidos como KDCs) y un número potencial de clientes.

keytab

Un fichero que incluye una lista desencriptada de "principals" y sus claves. Los servidores recuperan las claves que necesitan del fichero keytab en lugar de usar `kinit`. `/etc/krb5.keytab` es el fichero keytab por defecto. El comando `kadmind` es el único servicio que usa cualquier otro archivo (`/var/kerberos/krb5kdc/kadm5.keytab`)

principal

Usuario o servicio que puede autentificar mediante el uso de Kerberos. Un nombre de principal está en el formato "*root*[/*instance*]*@REALM*". Para un usuario típico, el *root* es igual a su ID de login. El *instance* es opcional. Si el principal tiene un instance, se separa del root con ("/"). Una cadena vacia ("") es un instance válido (que difiere del instance por defecto *NULL*), pero usarlo puede ser confuso. Todos los principals de un dominio tienen su propia clave, que se deriva de su contraseña (para usuarios) o aleatoriamente (para servicios)

servicio

Programa u ordenador al que se accede en la red.

texto cifrado

datos encriptados

texto sin retocar

Datos no encriptados.

ticket

Grupo temporal de credenciales electrónicas que verifica la identidad de un cliente para un servicio particular.

Ticket Granting Service (TGS)

Emite tickets para un servicio deseado que usa el usuario para ganar acceso al servicio. El TGS se ejecuta en el mismo host que KDC.

Ticket Granting Ticket (TGT)

Ticket especial que permite al cliente obtener tickets adicionales sin aplicarlos desde KDC.

10.4. Modo en que funciona Kerberos

Ahora que ya conoce algunos de los términos que utiliza Kerberos, aquí tiene una explicación del funcionamiento del sistema de autenticación Kerberos:

En lugar de la autenticación que ocurre entre cada máquina cliente y cada servidor, Kerberos usa la encriptación simétrica y una tercera parte de confianza — conocida como el Key Distribution Center o KDC — para autentificar usuarios en una red para un paquete de servicios en una red. Una vez autentificados, Kerberos guarda un ticket específico para esa sesión en la máquina del usuario y cualquier servicio kerberizado buscará este ticket en lugar de pedir al usuario que se identifique usando una contraseña.

Cuando un usuario en una red kerberizada se registra en su estación de trabajo, su principal se envía al Key Distribution Center (KDC) como una demanda para un Ticket Granting Ticket (TGT). Esta demanda puede ser enviada por el programa login (para que sea transparente al usuario) o puede ser enviada por el programa `kinit` después de que el usuario se registre.

El KDC verifica el principal en su base de datos. Si lo encuentra, el KDC crea un TGT, lo encripta usando las claves del usuario y lo devuelve al usuario.

El programa login en la máquina del cliente o `kinit` desencripta el TGP usando las claves del usuario (que computa de la contraseña del usuario). El TGT, que caduca después de un cierto período de tiempo, es almacenado en su caché de credenciales. Solo se puede usar un cierto períiodo de tiempo que suele ser de ocho horas. Esto es más seguro que un modelo de contraseña tradicional porque la contraseña nunca se pasa a través de la red. Una vez que se ha emitido el TGT, el usuario no tiene que introducir su contraseña en el KDC otra vez hasta que el TGT caduque o se desconecte y vuelva a conectarse.

Cuando el usuario necesita acceder a un servicio de red, el cliente usa el TGT para pedir un ticket para el servicio de Ticket Granting Service (TGS), que se ejecuta en el KDC. El TGS emite un ticket por el servicio deseado, que se usa para autentificar el usuario.

Como es de suponer la explicación es demasiado simplificada. Si necesita una explicación más detallada sobre el funcionamiento de kerberos, vea la Sección 10.8.

Nota

Kerberos depende de ciertos servicios de la red para trabajar correctamente. Primero, Kerberos necesita una sicronización de reloj entre los ordenadores y su red. Si no ha configurado un programa de sincronización de reloj para su red, como por ejemplo `ntpd`, deberá hacerlo. Ya que ciertos aspectos de kerberos se apoyan en el Domain Name System (DNS), debe de asegurarse de que las entradas DNS y los hosts en su red están configuradas correctamente. Vea la *Guía del administrador kerberos V5*, proporcionada en formatos PostScript y HTML, en `/usr/share/doc/krb5-server-<version-number>/`, si necesita más información sobre estos temas.

10.5. Kerberos y Pluggable Authentication Modules (PAM)

Actualmente, los servicios Kerberizados no hacen uso de PAM — un servidor kerberizado omite PAM completamente. Las aplicaciones que usan PAM pueden hacer uso de Kerberos para comprobar las contraseñas si el módulo `pam_krb5`pam_krb5 module (proporcionado en el `pam_krb5`) es instalado. El paquete `pam_krb5` contiene un ejemplo de ficheros de configuración que permiten servicios como `login` y `gdm` para autentificar usuarios y obtener credenciales iniciales usando sus contraseñas. Si el acceso a servicios de red siempre se realiza mediante servicios kerberizados (o servicios que usan GSS-API, como IMAP), la red puede ser considerada razonablemente segura.

Los administradores de sistemas cuidadosos no añaden verificación de contraseñas Kerberos a los servicios de la red, porque la mayoría de los protocolos usados por estos servicios no encriptan la contraseña antes de enviarla a través de la red.

10.6. Configuración de un servidor Kerberos 5

Antes de configurar un servidor Kerberos tiene que instalarlo. Si necesita instalar servidores esclavos, consulte el *Manual de instalación del Kerberos 5* que se encuentra en el directorio `/usr/share/doc/krb5-server-<version-number>`.

Para instalar un servidor Kerberos, siga los pasos siguientes:

1. Asegúrese de que tanto el reloj como el DNS funcionan correctamente en el servidor antes de configurar el Kerberos 5. Preste especial atanción a la sincronización de la hora del servidor Kerberos y de sus diversos clientes. Si la sincronización de los relojes del servidor y de los clientes se diferencia en más de cinco minutos (la cantidad predeterminada es configurable en el Kerberos 5), los clientes de Kerberos no podrán autentificar el servidor. La sincronización de los relojes es necesaria para evitar que un intruso use un ticket viejo de Kerberos para hacerse pasar como un usuario autorizado.

   Configure el protocolo cliente/servidor Network Time Protocol (NTP) con Red Hat Linux, aunque no está usando Kerberos. La Red Hat Linux 8.0 incluya el paquete `ntp` para facilitar la instalación. Consulte http://www.eecis.udel.edu/~ntp para mayor información sobre el protocolo NTP.

2. Instale los paquetes `krb5-libs`, `krb5-server` y `krb5-workstation` en la máquina en la vaya a ejecutar el KDC. Esta máquina tiene que ser segura, no podrá ejecutar otros servicios que no sean del KDC.

   Si desea utilizar la interfaz gráfica del usuario (GUI)para administrar Kerberos, tiene que instalar el paquete `gnome-kerberos`. Contiene `krb5`, una herramienta GUI para administrar tickets.

3. Modifique los ficheros de configuración `/etc/krb5.conf` y `/var/kerberos/krb5kdc/kdc.conf` para reflejar el nombre del dominio y los mappings de los dominios. Se puede crear un realm sustituyendo las instancias de *`EXAMPLE.COM`* y *`example.com`* con el nombre de su dominio — siempre y cuando se respete el formato

correcto de los nombres escritos en mayúscula y en minúscula — y se cambie el KDC del *`kerberos.example.com`* con el nombre de su servidor Kerberos. En general, los nombres de los realms están escritos en mayúscula y los nombres de las máquinas DNS y los nombres de los dominios van en minúscula. Para mayor información sobre los formatos de estos ficheros, consulte las páginas man correspondientes.

4. Cree la base de datos usando la utilidad `kdb5_util` en la shell del prompt:
   ```
   /usr/kerberos/sbin/kdb5_util create -s
   ```
   El comando `create` crea la base de datos que se usará para almacenar las claves del realm del Kerberos. El comando `-s` fuerza la creación del fichero *stash* en el que se almacena la clave del servidor master. Si no existe este último fichero, el servidor Kerberos(`krb5kdc`) pedirá al usuario la contraseña del servidor master, que se puede usar para regenerar la clave, cada vez que se arranque.

5. Modifique el fichero `/var/kerberos/krb5kdc/kadm5.acl`. Este fichero lo usa el comando `kadmind` para determinar qué usuarios principales tienen acceso a la base de datos de BKerberos y cuál es el nivel de acceso. La mayor parte de las organizaciones pueden acceder con una sola línea:
   ```
   */admin@EXAMPLE.COM  *
   ```
   La mayor parte de los usuarios aparecen en la base de datos como usuarios principales (la instancia *NULL*, aparece vacía, o contiene por ejemplo lo siguiente *joe@EXAMPLE.COM*). Con esta configuración los usuarios que tengan una segunda entrada como usuarios principales de *admin* (por ejemplo, *joe/admin@EXAMPLE.COM*) tendrán todo el acceso a la base de datos del realm de Kerberos.

   Una vez que se ejecuta el comando `kadmind` en el servidor, todos los usuarios tienen acceso a los servicios de este servidor ejecutando los comandos `kadmin` en cualquiera de los clientes o servidores del realm. Sin embargo, solamente los usuarios que aparecen en la lista del fichero `kadm5.acl` podrán modificar la base de datos salvo sus contraseñas.

   Nota

   Las utilidades `kadmin` se comunican con el servidor `kadmind` por la red y usan Kerberos para llevar a cabo la autentificación. Tiene que ser usuario principal antes de conectarse al servidor con la red para poder administrarla. Puede crear esta primera entrada con el comando `kadmin.local` el cual se ha creado específicamente para usarlo en la misma máquina que el KDC y no usa Kerberos para la autenticación.

   Escriba el comando `kadmin.local` en una terminal KDC para crear la primera entrada como usuario principal:
   ```
   /usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
   ```

6. Arranque Kerberos usando los siguientes comandos:
   ```
   /sbin/service krb5kdc start
   /sbin/service kadmin start
   /sbin/service krb524 start
   ```

7. Añada entradas para otros usuarios con el comando `addprinc` y `kadmin`. `kadmin` y `kadmin.local` en el KDC master son una línea de comandos que permite conectarse al sistema de administración de Kerberos. Para ello, existen otros comandos disponibles una vez que se ha lanzado el programa `kadmin`. Consulte las páginas man de `kadmin` para mayor información.

8. Verifique que el servidor crea tickets. Primero, ejecute `kinit` para obtener un ticket y alamacénelo en un fichero de credenciales caché. Después use el comando `klist` para visualizar la lista de credenciales en el caché y use el comando `kdestroy` para eliminar el caché y los credenciales que contenga.

Nota

Normalmente,`kinit` intenta autenticar el usuario usando el nombre de conexión de la cuenta que usó cuando se conectó al sistema (no al servidor Kerberos). Si ese nombre no corresponde al nombre de entrada principal, verá un mensaje que le indicará que hay un error. Si ocurre esto. simplemente, de al comando `kinit` el nombre de la entrada principal como argumento en la línea de comandos (`kinit` *`principal`*).

Si ha seguido estos pasos, el servidor Kerberos funcionará correctamente. Lo siguiente que tiene que hacer es configurar el cliente de Kerberos.

10.7. Configuración de un cliente de Kerberos 5

La configuración de un cliente de Kerberos 5 client no es tan complicada como la de un servidor. Lo que tiene que hacer es instalar los paquetes del cliente y proveer a cada cliente con un fichero de configuración `krb5.conf` válido. Las versiones kerberizadas de `rsh` y `rlogin` requerirán algunos cambios en la configruación.

1. Asegúrese que la sincronización sea correcta entre el cliente de Kerberos y el KDC. Consulte la Sección 10.6 para mayor información. Además, el DNS tiene que funcionar correctamente antes de instalar los programas del cliente Kerberos .
2. Instale los paquetes `krb5-libs` y `krb5-workstation` en todos las máquinas de clientes. Tiene que dar la versión del `/etc/krb5.conf` para cada cliente; normalmente es el mismo `krb5.conf` que usa el KDC.
3. Antes de que una estación de trabajo del realm permita a los usuarios conestarse usando los comandos kerberizados `rsh` y `rlogin`, la estación de trabajo tendrá que tener instalado el paquete `xinetd` y tener su propio nombre del host en la base de datos de Kerberos. Los programas del servidor `kshd` y `klogind` también necesitan el acceso a las claves de la entrada principal del servicio.

   Usando el comando `kadmin`, añada entradas para la estación de trabajo en el KDC. La instancia en este caso será el nombre del host de la estación de trabajo. Use la opción `-randkey` y el comando del kadmin `addprinc` *en el KDC* para crear una entrada principal y asignarla a una clave cualquiera:
   ```
   addprinc -randkey host/blah.example.com
   ```
   Ahora que ya ha creado la entrada principal, puede extraer las claves para la estación de trabajo ejecutando `kadmin` *en la estación de trabajo* y usando el comando `ktadd` en `kadmin`:
   ```
   ktadd -k /etc/krb5.keytab host/blah.example.com
   ```
   Para poder usar las versiones kerberizadas de los comandos `rsh` y `rlogin`, tiene que habilitar `klogin`, `eklogin` y `kshell`. [1]
4. Se tienen que arrancar otros servicios de red kerberizados. Para usar el comando kerberizado `telnet`, habilite `krb5-telnet`.

   Para el acceso FTP, cree y extraiga la calve para la entrada principal con un root de ftp, con las instancias que tenga que configurar para el servidor FTP. Habilite el comando `gssftp`.

   El servidor IMAP incluye el paquete `imap` que usará la autenticación GSS-API del Kerberos 5 si encuentra la calve adecuada en `/etc/krb5.keytab`. El root para la entrada principal tiene que ser `imap`. El servidor CVS usa una entrada principal con un root del `cvs` y es idéntica a `pserver`.

1. Consulte el capítulo *Control del acceso a los servicios* en el *Manual oficial de personalización de Red Hat Linux* para mayor información.

10.8. Recursos adicionales

Kerberos representa un desafío para los nuevos usuarios a la hora de entenderlo, implementarlo y configurarlo. Remítase a las siguientes fuentes de información, si desea tener más ejemplos e instrucciones sobre el uso de Kerberos:

10.8.1. Documentación instalada

- `/usr/share/doc/krb5-server-<version-number>` — La *Guía de instalación de Kerberos V5* y la *Guía del administrador del sistema Kerberos V5*, en formato PostScript y HTML, instaladas por el RPM `krb5-server`.
- `/usr/share/doc/krb5-workstation-<version-number>` — La *Guía del usuario UNIX de Kerberos V5*, en formato PostScript y HTML, instalada por el RPM `krb5-workstation`.

10.8.2. Sitios Web útiles

- http://web.mit.edu/kerberos/www — Página inicial de Kerberos en el sito Web MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — Preguntas más frecuentes sobre Kerberos (FAQ).
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — Enlace a una versión PostScript de *Kerberos: An Authentication Service for Open Network Systems* de Jennifer G. Steiner, Clifford Neuman y Jeffrey I. Schiller. Documento original que describe Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* originariamente de Bill Bryant en 1988, modificado por Theodore Ts'o en 1997. Este documento es una conversación entre dos diseñadores que están pensando la creación de un sistema de autenticación Kerberos. El estilo desenfadado de esta conversación lo convierte en un buen material para aquéllos que no tienen ningún tipo de familiaridad con Kerberos.
- http://www.ornl.gov/~jar/HowToKerb.html — *Cómo kerberizar su página.*
- http://www.networkcomputing.com/netdesign/kerb1.html — *Kerberos Network Design Manual* es una vista general al sistema Kerberos.

Capítulo 11.

Tripwire

El software Tripwire puede ayudarle a asegurar la integridad de ficheros y directorios de sistema esenciales identificando todos los cambios hechos a ellos. Las opciones de configuración de Tripwire incluyen la capacidad de recibir alertas por medio de correo electrónico si hay ficheros específicos que han sido modificados y el control de integridad automatizado a través de un trabajo `cron`. El uso de Tripwire para detectar intrusiones y fijar daños le ayuda a mantenerlo al tanto de los cambios del sistema y puede agilizar el restablecimiento de una entrada forzada reduciendo el número de ficheros que hay que restablecer para reparar el sistema.

Tripwire compara los ficheros y directorios con una base de datos de la ubicación de los ficheros, las fechas en que han sido modificados y otros datos. Tripwire genera la base tomando una instantánea de ficheros y directorios específicos en estado conocido como seguro. (Para máxima seguridad, Tripwire debería ser instalado y la base debería ser creada antes que el sistema sea expuesto al riesgo de intrusión.) Después de haber creado la base de datos de base, Tripwire compara el sistema actual con la base y proporciona información sobre cualquier modificación, añadidura, o supresión.

Aunque es una herramienta muy valiosa para revisar el estado de seguridad de su sistema, Tripwire no está soportada por Red Hat, Inc.. Contacte Tripwire, Inc., (http://www.tripwire.com) para consultar las opciones de soporte.

11.1. Cómo usar Tripwire

El siguiente diagrama de flujo ilustra cómo debería usarse Tripwire:

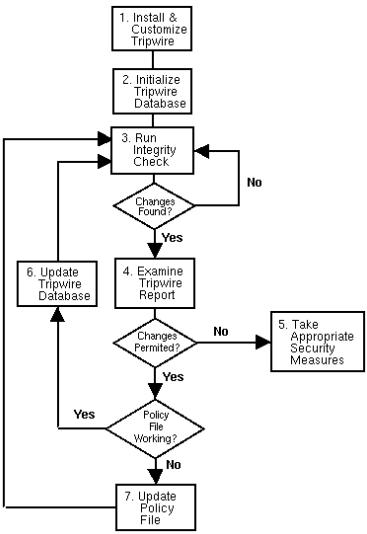

Figura 11-1. Cómo usar Tripwire

Los pasos a tomar para instalar, usar y mantener Tripwire adecuadamente son los siguientes (vea Figura 11-1:

1. *Instale Tripwire y personalice el fichero de política* — si no lo ha hecho ya, instale el RPM de `tripwire` (vea la Sección 11.2). Luego personalice la configuración de muestra (`/etc/tripwire/twcfg.txt`) y los ficheros de política (`/etc/tripwire/twpol.txt`) y ejecute la secuencia de comandos (`/etc/tripwire/twinstall.sh`). Consulte la Sección 11.3 para obtener más información.
2. *Inicialice la base de datos de Tripwire* — construya una base de datos de los ficheros de sistema esenciales para supervisarlos basándose en el contenido del fichero de política Tripwire nuevo y firmado (`/etc/tripwire/tw.pol`). Consulte la Sección 11.4 para obtener más información.
3. *Ejecute un control de integridad Tripwire* — compare la base de datos Tripwire recién creada con los ficheros de sistema reales en busca de ficheros modificados o desaparecidos. Consulte la Sección 11.5 para obtener más información.
4. *Examine el fichero de informes Tripwire* — Examine el fichero de informes Tripwire con `/usr/sbin/twprint` para distinguir las violaciones a la integridad. Consulte la Sección 11.6.1 para obtener más información.
5. *Tome las medidas de seguridad adecuadas* — si los ficheros bajo supervisión han sido modificados en modo inadecuado, los puede reemplazar con los originales salvados en copias de seguridad o reinstalar el programa.
6. *Actualice el fichero de la base de datos de Tripwire* — si las violaciones a la integridad son intencionales y válidas, como si usted hubiese intencionalmente modificado un fichero o reemplazado un determinado programa, debería avisarle al fichero de base de datos de Tripwire que no lo indique como violación en informes futuros. Consulte la Sección 11.7 para obtener más información.
7. *Actualice el fichero de política Tripwire* — si necesita cambiar la lista de ficheros que Tripwire supervisa, o la manera en que trata las violaciones a la integridad, debería actualizar su fichero de muestra de política (`/etc/tripwire/twpol.txt`), regenerar una copia firmada (`/etc/tripwire/tw.pol`), y actualizar su base de datos de Tripwire. Consulte la Sección 11.8 para obtener más información.

Consulte las secciones adecuadas en este capítulo para obtener instrucciones detalladas sobre estos pasos.

11.2. Instrucciones para la instalación de RPM

La forma más fácil de instalar Tripwire es instalando el RPM de `tripwire` durante el procedimiento de instalación de Red Hat Linux 8.0. Sin embargo, si ya había instalado Red Hat Linux 8.0, puede usar **rpm** o **Herramienta de gestión de paquetes** (`redhat-config-packages`) para instalar el RPM de Tripwire con los CD-ROMs de Red Hat Linux 8.0.

Si no está seguro de si ha instalado Tripwire is installed, escriba el siguiente comando en el indicador de comandos de la shell:

```
rpm -q tripwire
```

Si está instalado, aparecerá lo siguientes en la pantalla:

```
tripwire-<version-number>
```

Las siguientes pautas le dicen cómo encontrar e instalar el Tripwirw desde los CD-ROMs usando la línea de comandos de RPM:

1. Introduzac el *CD 2* de instalación de of the Red Hat Linux 8.0.
2. Si no se monta automáticamente el CD-ROM, escriba lo siguiente: command:
   `mount /mnt/cdrom`
3. Verique que el RPM `tripwire` se encuentra en el CD-ROm escribiendo:
   `ls /mnt/cdrom/RedHat/RPMS/ | grep tripwire`

   Si el RPM está en el CD-ROM, este comando le mostrará el nombre del paquete.

   Si el RPM *no* está en el CD-ROM, aparecerá de nuevo el indicador de comandos de la shell. En este caso, tiene que verificar el *CD 3* y, si es posible, también el *CD 1* de instalación de Red Hat Linux 8.0 desmontando el CD-ROM y siguiendo los pasos del 1 la tres con cada uno de los CD-ROMs.

   Desmonte el CD-ROM haciendo click con el botón derecho del reatón en el icono del CD-ROM y seleccionando **Sacar** o escribiendo el siguiente comando en el indicador de comandos de la shell:
   `umount /mnt/cdrom`
4. Una vez localizado el RPM `tripwire`, instálelo escribiendo el siguiente comando como usuario root:
   `rpm -Uvh /mnt/cdrom/RedHat/RPMS/tripwire*.rpm`

En el directorio `/usr/share/doc/tripwire-<version-number>/`, encontrará las notas de última hora y los ficheros README del Tripwire. Estos documentos contienen información importante sobre el fichero de política y otros temas.

11.3. Personalización de Tripwire

Después de haber instalado el RPM Tripwire, tiene que completar los siguientes pasos para inicializar el software:

11.3.1. Modificar `/etc/tripwire/twcfg.txt`

Aunque no tiene que modificar este fichero de prueba de configuración de Tripwire, le recomendamos que lo haga. De hecho, quizás desee alterar la localización de los ficheros Tripwire, personalizar los parámetros del e-mail o el nivel de detalles para los informes.

Debajo se exppone una lista con las variables configurables de usuario *requeridas* en el fichero `/etc/tripwire/twcfg.txt`:

- `POLFILE` — Especifica la localización del fichero de política; `/etc/tripwire/tw.pol` es el valor perdeterminado.
- `DBFILE` — Especifica la localización del fichero de la base de datos; `/var/lib/tripwire/$(HOSTNAME).twd` es el valor predeterminado.
- `REPORTFILE` — Especifica la localización de los ficheros de informe. Por defecto, el valor está en `/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr`.
- `SITEKEYFILE` — Especifica la localización del fichero de la llave del sitio; `/etc/tripwire/site.key` es el valor predeterminado.
- `LOCALKEYFILE` — Especifica la localización del fichero de la llave local; `/etc/tripwire/$(HOSTNAME)-local.key` es el valor predeterminado.

Importante

Si modifica el fichero de configruación y no define las variables anteriores, el fichero de configuración no será válido. So ocurre esto, cuando ejecute el comando `tripwire` aparecerá un mensaje de error y saldrá de la pantalla.

El resto de las vcaraibles del fichero de muestra `/etc/tripwire/twcfg.txt` son opcionales. Entre ellas se encuentran las siguientes:

- `EDITOR` — Especifica el editor de texto de Tripwire. El valor predeterminado es `/bin/vi`.
- `LATEPROMPTING` — Si es `verdadero` esta variable configura Tripwire de manera que espere el mayor tiempo posible antes de pedir la contraseña al usuario, minimizando así el tiempo que la contraseña permanece en la memoria. El valor predeterminado es `falso`.
- `LOOSEDIRECTORYCHECKING` — Si es `verdadero` esta variable configura Tripwire para que informe sobre los cambios que se han realizado en un fichero de un directorio y no sobre los cambios propios del directorio. Esto limita la redundancia en los informes de Tripwire. El valor predeterminado es `falso`.
- `SYSLOGREPORTING` — Si es `verdadero`, esta variable configura Tripwire para informe al demonio syslog con la facilidad del "usuario". El nivel de conexión está en `aviso`. Vea la página man de `syslogd` para mayor información. El valor predeterminado es `falso`.
- `MAILNOVIOLATIONS` — Si es `verdadero` esta variable configura Tripwire para que mande un informe en forma de e-mail a intervalos regulares sin tener en cuenta si se han producido violaciones. El valor predeterminado es `verdadero`.
- `EMAILREPORTLEVEL` — Especifica el nivel de detalles de los informes mandados por e-mail. Los valores válidos para esta variable son de `0` a `4`. El valor predeterminado es `3`.
- `REPORTLEVEL` — Especifica el nivel de detalles de los informes generados por el comando `twprint`. Este valor se puede cambiar en la línea de comandos pero el valor predeterminado es `3`.
- `MAILMETHOD` — Especifica qué protocolo de correo debe usar Tripwire. Los valores válidos son `SMTP` y `SENDMAIL`. El valor predeterminado es `SENDMAIL`.
- `MAILPROGRAM` — Especifica qué tipo de programa de correo debe usar Tripwire. El valor predeterminado es `/usr/sbin/sendmail -oi -t`.

Después de modificar el fichero de configuración de muestra, tiene que configurar el fichero de política de muestra.

Advertencia

Por razones de seguridad, debe de borrar o meter en un lugar seguro las copiar en texto del fichero `/etc/tripwire/twcfg.txt` después de ejecutar el script de instalación o regenerar un fichero de configuración firmado. También puede cambiar los permisos de manera que no se pueda leer.

11.3.2. Modificar `/etc/tripwire/twpol.txt`

Aunque no se requiere, debe de modificar este fichero de política para darse cuenta de las aplicaciones específicas, de los ficheros y de los directorios del sistema. Si confía en una configuración de muestra RPM el sistema no estará protegido.

La modificación del fichero de política aumenta la utilidad de los informes de Tripwire minimizando los avisos falsos para los ficheros y programas que no está usando y añade funcionalidad como por ejemplo las notificaciones en forma de e-mail.

Nota

La notificación via email no está configurada por defecto. Vea Sección 11.8.1 para mayor información.

Si modifica el fichero de política después de ejecutar el script de configuración, vea Sección 11.8 para saber cómo regenerar un fichero de política firmado.

Advertencia

Por razones de seguridad, debe de borrar o meter en un lugar seguro las copiar en texto del fichero `/etc/tripwire/twpol.txt` después de ejecutar el script de instalación o regenerar un fichero de configuración firmado. También puede cambiar los permisos de manera que no se pueda leer.

11.3.3. Ejecutar el script `twinstall.sh`

Teclee `/etc/tripwire/twinstall.sh` en la línea de comandos como root para ejecutar el script de configuración.la secuencia de comandos de configuración. La secuencia de comandos o script `twinstall.sh` le pedirá contraseñas locales y de sitios que se usan para generar llaves criptogáficas para los ficheros Tripwire. La secuencia de comandos crea y firma estos ficheros.

Cuando selecciona las contraseñas del sitio y las locales, tiene que tener en cuenta lo siguiente:

- Use al menos ocho caracteres alfanuméricos y simbólicos para cada una de las contraseñas peeo no exceda 1023.
- No las comillas en la contraseña.
- Las contraseñas Tripwire deben de ser diferentes de las de root o de cualquier otra contraseña del sistema.
- Use contraseñas únicas tanto para la clave del sitio como para la local.

>a contraseña de la clave del sitio protege la configuración de Tripwire y los ficheros de política. La contraseña dela clave local la base de datos de Tripwire y los ficheros de informes.

Advertencia

No se puede descifrar un fichero firmado si olvida su contraseña. Si ocurre esta situación, los ficheros son inservibles y tiene que ejecutar el script de configuración de nuevo.

Encriptando la configuración, los ficheros de política, la base de datos y los ficheros de informe, Tripwire los protege de los intrusos que no conocen las contraseñas locales no de los sitios. Esto siginifica que aunque un intruso obtenga al acceso de root al sistema, no podrá alterar los ficheros Tripwirw para enmascararse.

Una vez encriptados y firmados, no se puede cambiar el nombre ni mover los ficheros de configuración y de política generados con el script `twinstall.sh`.

11.4. Inicialización de la base de datos

Cuando Tripwire inicializa su base de datos, crea una colección de objetos de sistema de ficheros basada en las reglas en el fichero de política. Esta base de datos funciona como la línea base para controles de integridad.

Utilice el siguiente comando para inicializar la base de datos de Tripwire:

```
/usr/sbin/tripwire --init
```

Este comando puede tardar varios minutos en ejecutarse.

Una vez que ha seguido correctamente estos pasos, Tripwire tiena la instantánes del sistema de ficheros necesaria para verificar los cambios que se realicen en los ficheros importantes. Después de inicializar la base de datos de Tripwire, tiene que ejecutar una primera verificación de la integridad. La tiene que realizar antes de conectar el ordenador a la red. Para mayor información vea Sección 11.5.

Una vez que ha configurado Tripwire, ya puede poner el sistema en marcha.

11.5. Ejecución de un control de integridad

Por defecto, el RPM Tripwire añade un script de la shell llamado `tripwire-check` al directorio `/etc/cron.daily/`. Esto automáticamente ejecuta el control de la integridad uan vez al día.

Sin embargo, puede ejecutar el control de la integridad Tripwirw en cualquier momento escribiendo el siguiente comando:

```
/usr/sbin/tripwire --check
```

Cuando ejecuta un control de integridad, Tripwire compara los objetos de sistema de ficheros actuales y reales con sus propiedades como han sido indicadas en su base de datos. Las violaciones se imprimen a una salida estándar y se guardan en un fichero de informe al cual se pueda tener acceso más tarde mediante `twprint`. Para obtener más información sobre la lectura de informes Tripwire, vea la Sección 11.6.1.

Una opción de configuración de correo electrónico en el fichero de política permite además que determinadas direcciones de correo electrónico reciban avisos cuando ocurren ciertas violaciones a la integridad. Consulte la Sección 11.8.1 para obtener instrucciones sobre cómo configurar esta opción.

11.6. Verificación de los informes Tripwire

El comando `/usr/sbin/twprint` se usa para visualizar los informes encriptados Tripwirw y las bases de datos.

11.6.1. Visualización de los informes Tripwire

El comando `twprint -m r` muestra el contenido de un informe Tripwire en texto sin cifrar. Usted debe decirle a `twprint` cuál informe poner en pantalla.

Un comando `twprint` para imprimir informes Tripwire sería semejante a lo siguiente (todo en una línea):

```
/usr/sbin/twprint -m r --twrfile /var/lib/tripwire/report/<name>.twr
```

La opción `-m r` en el comando le ordena a `twprint` que descifre el informe Tripwire. La opción `--twrfile` le ordena a `twprint` que use un fichero de informe Tripwire específico.

El nombre del informe Tripwire que desea ver contiene el nombre del host que Tripwire ha controlado para generar el informe, además de la fecha y hora de la creación. Usted puede consultar informes guardados previamente en cualquier momento. Simplemente teclee `ls /var/lib/tripwire/report` para ver una lista de informes Tripwire.

Los informes Tripwire pueden ser algo largos, según la cantidad de violaciones encontrada o los errores generados. Un informe de muestra empieza así:

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Fri Jan 12 04:04:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================================
Report Summary:
===============================================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
-------------------------------------------------------------------------------
  Rule Name                Severity Level    Added    Removed  Modified
  ---------                --------------    -----    -------  --------
  Invariant Directories    69                0        0        0
  Temporary directories    33                0        0        0
* Tripwire Data Files      100               1        0        0
  Critical devices         100               0        0        0
  User binaries            69                0        0        0
  Tripwire Binaries        100               0        0        0
```

11.6.2. El uso de `twprint` para ver la base de datos de Tripwire

También puede usar `twprint` para ver la base de datos entera o información sobre determinados ficheros en la base de datos Tripwire. Esto es útil para ver la cantidad de información Tripwire que está supervisando en su sistema.

Teclee este comando para ver la base de datos Tripwire entera:

```
/usr/sbin/twprint -m d --print-dbfile | less
```

Este comando genera una gran cantidad de salida, con las primeras línea parecidas a esto:

```
Tripwire(R) 2.3.0 Database

Database generated by:        root
Database generated on:        Tue Jan  9 13:56:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
```

```
Database Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --init

===============================================================
Object Summary:
===============================================================
---------------------------------------------------------------
# Section: Unix File System
---------------------------------------------------------------
     Mode        UID          Size       Modify Time
     ------      ----------   ---------- ----------
 /
     drwxr-xr-x  root (0)     XXX        XXXXXXXXXXXXXXXXX
 /bin
     drwxr-xr-x  root (0)     4096       Mon Jan  8 08:20:45 2001
 /bin/arch
     -rwxr-xr-x  root (0)     2844       Tue Dec 12 05:51:35 2000
 /bin/ash
     -rwxr-xr-x  root (0)     64860      Thu Dec  7 22:35:05 2000
 /bin/ash.static
     -rwxr-xr-x  root (0)     405576     Thu Dec  7 22:35:05 2000
```

Para ver información sobre un determinado fichero que Tripwire está supervisando, como `/etc/hosts`, teclee otro comando `twprint`:

```
/usr/sbin/twprint -m d --print-dbfile /etc/hosts
```

El resultado será algo parecido a esto:

```
Object name:  /etc/hosts

Property:               Value:
-------------           -----------
Object Type             Regular File
Device Number           773
Inode Number            216991
Mode                    -rw-r--r--
Num Links               1
UID                     root (0)
GID                     root (0)
```

Consulte la página de manual de `twprint` para conocer otras opciones.

11.7. Actualización de la base de datos después de un control de integridad

Si ejecuta un control de integridad y Tripwire encuentra violaciones, primero habrá que determinar si las violaciones detectadas son realmente brechas en la seguridad o el producto de modificaciones autorizadas. Si ha instalado recientemente una aplicación o ha modificado ficheros de sistema esenciales, Tripwire le informará (debidamente) de violaciones a la integridad. En este caso debería actualizar su base de datos Tripwire para que esos cambios no vuelvan a aparecer en los informes como violaciones. Sin embargo, si se efectúan cambios no autorizados a ficheros de sistema, generando violaciones al control de integridad, entonces debería restablecer el fichero original de una copia de seguridad o reinstalar el programa.

Para actualizar su base de datos de Tripwire de modo que acepte las violaciones encontradas en un informe, debe especificar el informe que desea usar para actualizar su base de datos. Cuando inicie un comando para integrar esas violaciones válidas en su base de datos, asegúrese de usar el informe más reciente. Teclee el siguiente comando (todo en una línea), donde *name* es el nombre del informe que deber usarse:

```
/usr/sbin/tripwire --update --twrfile
          /var/lib/tripwire/report/<name>.twr
```

Tripwire le mostrará el informe específico por medio del editor de textos predeterminado (especificado en el fichero de configuración Tripwire en la línea EDITOR). Ésta es su oportunidad para quitar de la selección ficheros que no desea que se actualicen en la base de datos de Tripwire. Es importante que permita que sólo se cambien las violaciones autorizadas a la integridad en la base de datos.

Todas las actualizaciones propuestas a la base de datos de Tripwire inician con una `[x]` antes del nombre del fichero como el siguiente ejemplo:

```
Added:
[x] "/usr/sbin/longrun"

Modified:
[x] "/usr/sbin"
[x] "/usr/sbin/cpqarrayd"
```

Si desea excluir específicamente que una violación válida sea añadida a la base de datos de Tripwire, quite la `x` de la casilla. Para aceptar como cambio cualquier fichero con la `x` al lado, escriba el fichero en el editor y salga del editor de textos.

Para modificar el editor predeterminado de Tripwire,`vi` escriba el comando `i` y pulse [Intro] para efectuar los cambios a la base de datos de Tripwire. Cuando acabe, pulse [Esc], `:wq`, e [Intro]. Se le pedirá que teclee contraseña local de manera que la base de datos se vuelve a crear con los cambios y se vuelve a firmar.

Después de que se haya escrita una nueva base de datos de Tripwire, las violaciones a la integridad recién integradas no volverán a aparecer como advertencias cuando se ejecute el siguiente control de integridad.

11.8. Actualización del fichero de política

Si en realidad desea modificar los ficheros que Tripwire escribe en su base de datos o modificar la severidad con la cual se informan las violaciones, necesita modificar su fichero de política Tripwire.

Primero haga todos los cambios necesarios en el fichero de política de muestra (`/etc/tripwire/twpol.txt`). Si lo borró puede regenerarlo con el comando:

```
twadmin --print-polfile > /etc/tripwire/twpol.txt
```

Un cambio común a este fichero de política es convertir en comentario cualquier fichero que no existe en su sistema para que no genere un mensaje de error de `file not found` en los informes de Tripwire. Si por ejemplo su sistema no contiene un fichero `/etc/smb.conf`, puede decirle a Tripwire que no intente buscarlo a través de la conversión de su línea en comentario en `twpol.txt`:

```
#     /etc/smb.conf                     -> $(SEC_CONFIG) ;
```

Luego debe decirle a Tripwire que genere un fichero nuevo `/etc/tripwire/tw.pol` firmado y después que genere un fichero de base de datos actualizado basado en esta información de política. Suponiendo que `/etc/tripwire/twpol.txt` es el fichero de política modificado, use este comando:

```
/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Se le pedirá la frase de contraseña de sitio. Luego el fichero `twpol.txt` se analizará sintácticamente y se firmará.

Es importante actualizar la base de datos de Tripwire después de haber creado un fichero `/etc/tripwire/tw.pol` nuevo. La forma más confiable para llevarlo a cabo es borrando su base de datos de Tripwire actual y creando una base de datos nueva con el fichero de política nuevo.

Si su fichero de base de datos de Tripwire se llama `bob.domain.com.twd`, teclee este comando:

```
rm /var/lib/tripwire/bob.domain.com.twd
```

Luego teclee el comando para crear una base de datos nueva:

```
/usr/sbin/tripwire --init
```

Para asegurarse que la base de datos haya sido modificada correctamente, ejecute manualmente el primer control de integridad y vea el contenido del informe consiguiente. Consulte la Sección 11.5 y la Sección 11.6.1 para obtener instrucciones específicas sobre estas cuestiones.

11.8.1. Tripwire y el correo electrónico

Tripwire puede enviar un mensaje de correo electrónico a alguien si se ha violado un tipo específico de regla en el fichero de política. Para configurar Tripwire de manera que haga esto, primero hay que saber la dirección de correo electrónico de la persona que recibirá el mensaje si ocurre un determinado tipo de violación a la integridad, además del nombre de la regla que desea supervisar. Nótese que en sistemas grandes con administradores múltiples, puede avisar diferentes conjuntos de personas para determinadas violaciones y no avisarle a nadie si ocurren sólo violaciones menores.

Una vez que se sabe a quién avisar y sobre qué avisar, añada la línea emailto= a la sección de directivas de reglas de cada regla. Hágalo añadiendo una coma después de la línea severity= y poniendo emailto= en la línea siguiente, seguida por las direcciones de correo electrónico a las cuales enviar los informes de violaciones a esa regla. Se enviarán mensajes de correo electrónico múltiples si más de una dirección de correo electrónico ha sido especificada y si están separadas por un punto y coma.

Si por ejemplo usted quisiera que a dos administradores, Sam y Bob, se les avise que se ha modificado el programa de red, cambie la directiva de la regla de Programas de Red en el fichero de política de esta manera:

```
(
  rulename = "Networking Programs",
  severity = $(SIG_HI),
  emailto = johnray@domain.com;bob@domain.com
)
```

Para obtener las instrucciones sobre cómo firmar su fichero de política, consulte la Sección 11.8.

11.8.1.1. Envío de mensajes de correo electrónico de prueba

Para asegurarse que la configuración para los avisos de correo electrónico por parte de Tripwire realmente sea capaz de enviar mensajes de correo electrónico correctamente, use el siguiente comando:

```
/usr/sbin/tripwire --test --email your@email.address
```

Se enviará inmediatamente un mensaje de correo electrónico de prueba a la dirección de correo electrónico por medio del programa `tripwire`.

11.9. Actualización del fichero de configuración de Tripwire

Si desea cambar el fichero de configuración de Tripwire, primero modificuqe el fichero de configuración de muestra `/etc/tripwire/twcfg.txt`. Si lo borró, lo puede regenerar con el siguiente comando:

```
twadmin --print-cfgfile > /etc/tripwire/twcfg.txt
```

Tripwire no reconocerá los cambios realizados hasta que el fichero de texto de configuración está firmado correctamente y se haya convertido al `/etc/tripwire/tw.pol` con el comando `twadmin`.

Use el siguiente comando para regenerar el fichero de configuración del fichero de texto `/etc/tripwire/twcfg.txt`:

```
/usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Debido a que el fichero de configuración no altera las políticas de Tripwire o los ficheros reconocidos por la aplicación, no es necesario regenerar la base de datos de Tripwire.

11.10. Referencia de la localización del fichero Tripwire

Antes de trabajar con Tripwire, tiene que saber dónde están localizados los ficheros importante para la aplicación. Tripwirw almacena los ficheros en una serie de lugares dependiendo de la función que tengan.

- En el directorio `/usr/sbin/` se encuentran los siguientes programas:
  - `tripwire`
  - `twadmin`
  - `twprint`

- En el directorio `/etc/tripwire/` se encuentran los siguientes ficheros:
  - `twinstall.sh` — El script de inicialización para Tripwire.
  - `twcfg.txt` — El fichero de configruación de muestra que ofrece el RPM Tripwire.
  - `tw.cfg` — El fichero de configuración firmado creado por el script `twinstall.sh`.
  - `twpol.txt` — El fichero de política de muestra ofrecido por el RPM Tripwire.
  - `tw.pol` — El fichero de política firmado creado por el script `twinstall.sh`.

  - Ficheros claves — Las claves locales y del sitio creada por el script `twinstall.sh` que acaba con la extensión de fichero `.key`.

- Después de ejecutar el script de instalación `twinstall.sh` encontrará los siguientes ficheros en el directorio `/var/lib/tripwire/`:
  - La base de datos Tripwire — La base de datos de los ficheros del sistema que tiene la extensión de fichero `.twd`.
  - Informes Tripwire — El directorio `report/` es donde se almacenan los informes Tripwire.

La siguiente sección explica las funciones que estos ficheros desempeñas en el sistema Tripwire.

11.10.1. Componentes Tripwire

A continuación le exolicamos más detalladamente las funciones anteriormente descritas.

`/etc/tripwire/tw.cfg`

Es el fichero de configuración encriptadas de Tripwire que almacena la información específica del sistema como la localización de los ficheros de datos de Tripwirw. El script instaladortwinstall.sh y el comando `twadmin` generan este fichero usando la información de la versión en texto del fichero de configuración `/etc/tripwire/twcfg.txt`.

Después de ejecutar el script de instalación, el administrador de sistemas puede cambiar los parámetros modificando `/etc/tripwire/twcfg.txt` y regenerando una copia firmada del fichero `tw.cfg` usando el comando `twadmin`. Vea la Sección 11.9 para mayor información.

`/etc/tripwire/tw.pol`

El fichero de política activo de Tripwire es el fichero encriptado que contiene comentarios, reglas, directivas y variables. Este fichero dicta la manera en la que Tripwire verifica el sistema. Cada regal en el fichero de política especifica el sistema que se debe controlar. Las regasl también describen los cambios que se deben dar a conocer y los que no.

Los objetos del sistema son los ficheros y directorio s que desea controlar. Cada objeto se identifica con un nombre de objeto. Una propiedad se refiere a una sola característica de un objeto que el software Tripwire puede controlar. Las directivas controlan procesos adicionales de grupos de reglas en el fichero de política. Durante la instalación, el texto muestra del fichero de política, `/etc/tripwire/twpol.txt`, se usa para generar el fichero de política activo de Tripwire.

Después de ejecutar el script de instalación , el administrador del sistema puede actualizar el fichero de política de Tripwire modificando `/etc/tripwire/twpol.txt` y regenerando una copia firmada del fichero `tw.pol` con el comando `twadmin`. Vea la Sección 11.8 para mayor información.

`/var/lib/tripwire/host_name.twd`

Cuando inicializa por primera vez Tripwire, Tripwire usa las reglas del fichero de política firmado para crear este fichero de base de datos. La base de datos Tripwire es la instantánea del sitema en un estado seguro. Tripwire la compara con el sistema actual para determinar qué cambios se han producido. Se llama *control de integridad*.

`/var/lib/tripwire/report/host_name-date_of_report-time_of_report.twr`

Cuando lleva a cabo el control de integridad, Tripwire crea ficheros de informe en el directorio `/var/lib/tripwire/report/`. Los ficheros de informe resumen los cambios realizados

en loos ficheros que violaban las reglas de los ficheros de política durante el control de integridad. Los informes se nombran usando la siguiente convención: *`host_name-date_of_report-time_of_report`*`.twr`. Estos informes detallan las diferencias entre la base de datos Tripwire y los ficheros de su sistema.

11.11. Otros recursos

Tripwire es capaz de hacer más de lo que se cubre en este capítulo. Consulte estas fuentes de información adicionales para saber más sobre Tripwire.

11.11.1. Documentación instalada

- `/usr/share/doc/tripwire-<`*`version-number`*`>` — un excelente punto de inicio para aprender sobre cómo personalizar los ficheros de configuración y de política en el directorio `/etc/tripwire`.
- Consulte además las páginas de manual para `tripwire`, `twadmin` y `twprint` donde encontrará ayuda para el uso de estas utilidades.

11.11.2. Sitios web útiles

- http://www.tripwire.org — La sede del Tripwire Open Source Project (proyecto de open source de Tripwire), donde podrá encontrar las más recientes noticias sobre el programa, incluyendo una lista de FAQ.

Servicios de red

Capítulo 12.

Scripts de red

Usando Red Hat Linux, todas las comunicaciones de red acontecen entre *interfaces*, que son dispositivos de networking conectados al sistema, configurados de un modo determinado y usando un protocolo, al menos, para intercambiar datos con otros sistemas. Los diferentes tipos de interfaz que existen son tan variados como los dispositivos que los soportan.

Los ficheros de configuración para las diferentes interfaces de red y scripts para activarlos o desactivarlos están ubicados en el directorio `/etc/sysconfig/network-scripts`. Mientras que la existencia de ficheros de interfaces particulares puede diferir de sistema a sistema dependiendo del uso, los tres tipos de ficheros diferentes que existen en este directorio, *ficheros de configuración de interfaz*, *scripts de control de interfaz* y *ficheros de función de red*, funcionan conjuntamente para habilitar Red Hat Linux para el uso de diversos dispositivos de red disponibles.

Este capítulo explorará la relación entre estos ficheros y las diferentes opciones para su uso.

12.1. Ficheros de configuración de red

Antes de revisar los ficheros de configuración de interfaz estudiemos los ficheros de configuración principales que usa Red Hat Linux para configurar la red. La comprensión del papel que desemepeñan en la configuración de la red es fundamental para configurar el sistema.

Los principales ficheros de configuración de la red son los siguientes:

- `/etc/hosts` — El principal propóposito de este fichero es resolver los nombres de hosts que no se pueden resolver en otra manera. Se puede usar solamente para resolver nombres de hosts en pequeñas redes sin servidor DNS. Sin tener en cuenta el tipo de red que el ordenador use, este fichero contiene un línea que especifica la direcciól̀n IP del dispositivo loopback (`127.0.0.1`) como por ejemplo `localhost.localdomain`. Para mayor información consulte la página man del host.
- `/etc/resolv.conf` — Este fichero especifica las direcciones IP de los servidores DNS y el dominio de búsqueda. A menos que se haya configurado para algo diferente, los scripts de inicialización de la red llenan este fichero. Para mayor información consulte la página man resolv.conf.
- `/etc/sysconfig/network` — Especifica la información del routing y del host para todas las interfaces de red. Para mayor información sobre este fichero y las directivas que acepta consulte la Sección 3.7.1.23.
- `/etc/sysconfig/network-scripts/ifcfg-<interface-name>` — Para cada interfaz de red del sistema Red Hat Linux existe un script de configuración de interfaz para una interfaz de red determinada. Consulte la Sección 12.2 para mayor información.

Advertencia

El directorio `/etc/sysconfig/networking/` lo usa la herramienta **Herramienta de administración de red** (`redhat-config-network`) y sus contenidos no se modifican manualmente. Para mayor información sobre la configuración de las interfaces de red usando la herramienta **Herramienta de administración de red**, consulte el capítulo *Configuración de red* en el *Manual oficial de personalización de Red Hat Linux*.

12.2. Ficheros de configuración de interfaz

Los ficheros de configuración de interfaz controlan la operación de un dispositivo de interfaz de red particular. Cuando su sistema Red Hat Linux arranca, utiliza estos ficheros para saber qué interfaces utilizar automáticamente y cómo configurarlas para que operen correctamente. Estos ficheros habitualmente se conocen como `ifcfg-<device>`, donde `<device>` hace referencia al nombre del dispositivo que controla el fichero de configuración.

12.2.1. Interfaces Ethernet

Uno de los ficheros de interfaz más comunes es `ifcfg-eth0`, que controla el primer NIC de un sistema. En un sistema con muchos NICs, tendrá ficheros `ifcfg-eth` múltiples, cada uno con nun número al final del nombre del fichero. Como cada dispositivo tiene su propio fichero de configuración, llevará un gran control sobre el modo en que funciona cada interfaz.

Un ejemplo `ifcfg-eth0` para un sistema que usa una dirección IP fija sería de la siguiente manera:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Los valores que se requieren en un fichero de configuración de interfaz pueden cambiar basándose en otros valores. Por ejemplo, el fichero `ifcfg-eth0` para una interfaz que use DHCP aparecerá diferente, debido al hecho de que la información IP viene proporcionada por el servidor DHCP:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

La mayoría del tiempo, deseará utilizar una utilidad GUI, como por ejemplo **Configurador de red** (`redhat-config-network`) o `netconfig` para hacer cambios en los diversos ficheros de configuración de interfaz. Vea el *Manual oficial de personalización de Red Hat Linux* para más instrucciones sobre el uso de estas herramientas.

También puede modificar el fichero de configuración de un determinado dispositivo de red a mano. A continuación, le mostramos los parámetros que necesita para modificar el fichero de configuración.

Dentro de cada uno de los ficheros de configuración de la interfaz, son comunes los siguientes valores:

- `BOOTPROTO=<protocol>`, donde `<protocol>` es uno de los siguientes:
  - `none` — No se debería utilizar ningún protocolo de tiempo de arranque.
  - `bootp` — Se debería utilizar el protocolo BOOTP.
  - `dhcp` — Se debería utilizar el protocolo DHCP.

- `BROADCAST=<address>`, donde `<address>` es la dirección de broadcast.
- `DEVICE=<name>`, donde `<name>` es el nombre del dispositivo físico (a excepción de los dispositivos PPP asignados de forma dinámica donde es el *nombre lógico*).
- `DNS{1,2}=<address>`, donde `<address>` es la dirección del servidor de nombres que se tiene que colocar en `/etc/resolv.conf` si la directiva `PEERDNS` está activada.
- `IPADDR=<address>`, donde `<address>` es la dirección IP.

- `NETMASK=<mask>`, donde `<mask>` es el valor de la máscara de red.
- `NETWORK=<address>`, donde `<address>` es la dirección de red. Esta opción ya no se usa.
- `ONBOOT=<answer>`, donde `<answer>` es uno de los siguientes:
  - `sí` — El dispositivo debería activarse en el momento de arranque.
  - `no` — Este dispositivo no debería activarse en el momento de arranque.

- `PEERDNS=<answer>`, donde `<answer>` es uno de las siguientes:
  - `sí` — Modicar `/etc/resolv.conf` si la directiva DNS está activada. Si estáusando DCHP, la opción `sí` es la predeterminada.
  - `no` — No modificar `/etc/resolv.conf`.
  - `SRCADDR=<address>`, donde `<address>` es la dirección IP de una fuente específica para los paquetes externos.
  - `USERCTL=<answer>`, donde `<answer>` es uno de los siguientes:
    - `verdadero` — Se les permite controlar este dispostivo a todos los ususarios, aunque éstos no sean root.
    - `falso` — No se les permite controlar este dispositivo a los usuarios que no sean root.

12.2.2. Interfaces de acceso telefónico

Si se conecta a una red, como Internet, a través de la conexión de acceso telefónico PPP, necesitará un fichero de configuración para esa interfaz.

Este fichero se crea automáticamente cuando usa las aplicaciones `wvdial`, **Herramienta de administración de red** o **Kppp** para crear una cuenta telefónica. Además, todos los cambios que se hagan en la cuentas telefónica se reflejan en estos ficheros de configuración de estos dispositivos. El *Manual oficial del principiante de Red Hat Linux* contine las instrucciones para usar estas herramientas de conexión telefónica. También puede crear y modificar este fichero a mano. La muestra de ficheros `ifcfg-ppp0` sería de la siguiente manera:

```
DEVICE=ppp0
NAME=test
WVDIALSECT=test
MODEMPORT=/dev/modem
LINESPEED=115200
PAPNAME=test
USERCTL=true
ONBOOT=no
PERSIST=no
DEFROUTE=yes
PEERDNS=yes
DEMAND=no
IDLETIMEOUT=600
```

El *Protocolo de Internet de línea serial (SLIP)* es otra interfaz de acceso telefónico, aunque se usa menos. Los fichero SLIP tienen nombres de ficheros de configuración de interfaz tales como `ifcfg-sl0`.

Opciones que se pueden utilizar en estos ficheros:

- `DEFROUTE=<answer>`, donde `<answer>` es uno de las siguientes:
  - `sí` — Establece esta interfaz como la ruta por defecto.
  - `no` — No establece la interfaz como la ruta por defecto.

- `DEMAND=<answer>`, donde `<answer>` es una de las siguientes:
  - `sí` — Esta interfaz permitirá que `pppd` inicie una conexión cuando alguien está intentando utilizarla.
  - `no` — Se debe establecer una conexión de forma manual para esta interfaz.

- `IDLETIMEOUT=<value>`, donde `<value>` es el número de segundos de actividad improductiva antes de que la interfaz se desconecte.
- `INITSTRING=<string>`, donde `<string>` es la cadena init que pasa al dispositivo del módem. Esta opción se usa en primer lugar con las interfaces SLIP.
- `LINESPEED=<value>`, donde `<value>` es el ratio de baudios del dispositivo. Los posibles valores estándar incluyen `57600`, `38400`, `19200` y `9600`, entre otros.
- `MODEMPORT=<device>`, donde `<device>` es el nombre del dispositivo (habitualmente un módem) que se usa para establecer la conexión para la interfaz.
- `MTU=<value>`, donde `<value>` es la *unidad máxima de transferencia (MTU)* configurada para la interfaz. La MTU hace referencia a el mayor número de bytes de datos que puede abarcar un bloque, sin contar la información de encabezamiento y de final. En algunas situaciones de acceso telefónico, configurarlo hasta un valor de `576` dará un resultado de pocos paquetes eliminados y mejorará muy vagamente la capacidad de tratamiento para una conexión.
- `NAME=<name>`, donde `<name>` esla referencia al título que se le da al grupo de configuraciones de conexiones de acceso telefónico.
- `PAPNAME=<name>`, donde `<name>` es el nombre de usuario dado durante el intercambio del *Protocolo de autenticación de contraseña (PAP)* que le permite conectarse a un sistema remoto.
- `PEERDNS=<answer>`, donde `<answer>` es una de las siguientes:
  - `sí` — Esta interfaz modificará las entradas del fichero `/etc/resolv.conf` del sistema para el uso de los servidores DNS proporcionados por el sistema remoto cuando se establece una conexión.
  - `no` — El fichero `/etc/resolv.conf` no cambiará.

- `PERSIST=<answer>`, donde `<answer>` es una de las siguientes:
  - `sí` — Esta interfaz debería mantenerse siempre activa, incluso si se desactiva tras una detención del módem.
  - `no` — Esta interfaz no debería mantenerse siempre activa.

- `REMIP=<address>`, donde `<address>` es la dirección IP del sistema remoto. Habitualmente esto no se especifica.
- `WVDIALSECT=<name>`, donde `<name>` asocia esta interfaz con una configuración de marcado en `/etc/wvdial.conf`, que contiene el número de teléfono para que sea marcado y otra información importante para la interfaz.

12.2.3. Otras interfaces

Otro fichero de configuración de interfaz comunes que usan eestas opciones es el `ifcfg-lo`, que controla el dispositivo loopback local del protocolo IP, `ifcfg-irlan0`, que establece los parámetros para el primer dispositivo infrarojo, `ifcfg-plip0`, que controla el primer dispositivo PLIP, y `ifcfg-tr0`, que se usa con el primer dispositivo Token Ring.

A menudo se usa una *interfaz loopback* en las pruebas así como una variedad de aplicaciones que requieren una dirección IP que apunte al mismo sistema. Todos los datos que se mandan al dispositivo loopback vuelven inmediatamente a la red del host. layer.

Advertencia

No modifique nunca el script de la interfaz loopback `/etc/sysconfig/network-scripts/ifcfg-lo` manualmente. Si ocurre lo contrario, el sistema puede dejar de funcionar correctamente.

Una *interfaz de infrarojo* permite que se transmita información entre dispositivos como un portátil y una impresora y además se puede pasar a un enlace infrarojo que funciona como el dispositivo Ethernet excepto que se da en una conexión peer-to-peer.

La conexión *Parallel Line Interface Protocol (PLIP)* funciona de la misma manera, solamente que usa un paralelo. port.

Las topologías *Token Ring* no son tan frecuentes como las redes de área local como antes ocurría ya que han Ethernet las ha sustituido.

12.2.4. Ficheros alias y clon

Dos tipos menos usados de ficheros de configuración de interfaz que se encuentran en `/etc/sysconfig/network-scripts` son los ficheros *alias* y *clon*, que incluyen un componente adicional en el nombre del fichero más allá del nombre de la interfaz.

Los ficheros de configuración de la interfaz toman nombres en el formato de `ifcfg-<if-name>:<alias-value>` y permiten que un alias señale una interfaz. Por ejemplo, un fichero `ifcfg-eth0:0` podría estar configurado para especificar `DEVICE=eth0:0` y una dirección IP estática de 10.0.0.2, que sirva como un alias de una interfaz Ethernet que ya haya sido configuradad para recibir la información IP a través de DHCP en `ifcfg-eth0`. Llegado a ese punto, el dispositivo `eth0` está ligado a una dirección IP 10.0.0.2.

Un fichero de configuración de clon tiene un nombre parecido a `ifcfg-<if-name>-<clone-name>`. Un fichero alias es otro modo de referirse a un fichero de configuración de interfaz ya existente, mientras que un fichero clon se usa para especificar opciones adicionales al especificar una interfaz. Por ejemplo, si tiene una interfaz Ethernet DHCP estándar llamada `eth0`, será de la siguiente manera:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Como `USERCTL` no está configurado para la opción `sí`, los usuarios no pueden activar y desactivar esta interfaz. Para que los usuarios gocen de esta habilidad, cree un clon llamado `user` de `ifcfg-eth0` que permita que un usuario active o no la interfaz `eth0`. El nombre que resulta del clon sería `ifcfg-eth0-user` y tan sólo necesitaría una línea:

```
USERCTL=yes
```

Cuando un usuario activa la interfaz `eth0` mediante el comando `ifup eth0-user`, las opciones de configuración desde `ifcfg-eth0` y `ifcfg-eth0-user` se usan conjuntamente. Aunque este ejemplo es muy sencillo, este método puede ser utilizado con una variedad de opciones e interfaces.

El modo más sencillo de crear ficheros de configuración de interfaces alias y clon es mediante el uso de la herramienta **Herramienta de administración de red**. Para mayor información, consulte el capítulo *Configuración de red* en el *Manual oficial de personalización de Red Hat Linux*.

12.3. Scripts de control de interfaz

Los scripts de control de interfaz controlan la activación y desactivación de las conexiones de interfaz. Existen dos scripts de control de la interfaz primarios, `/sbin/ifdown` y `/sbin/ifup` que utilizan otros scripts de control variados localizados en el directorio `/etc/sysconfig/network-scripts` para activar y desactivar las interfaces de red.

Los dos scripts de control de interfaz son `ifdown` y `ifup` y son enlaces simbólicos para los scripts en el directorio `/sbin`. Cuando se solicita cualquiera de estos scripts, aceptan el uso de un valor de la interfaz, como por ejemplo:

```
ifup eth0
Determining IP information for eth0... done.
```

Tras haber verificado que se ha especificado una interfaz y que al usuario que ha ejecutado la petición se le permite activar o desactivar la interfaz, se solicita el script correcto para el tipo de dispositivo de interfaz. Los siguientes scripts de control de interfaz son los más habituales de este tipo:

- `ifup-aliases` — Configura los alias IP desde los ficheros de configuración de la interfaz cuando se asocia más de una dirección IP con una interfaz.
- `ifdown-cipcb` y `ifup-cipcb` — Se usan para activar y desactivar conexiones *Crypto IP Encapsulation (CIPE)*.
- `ifdown-ipv6` y `ifup-ipv6` — Contiene la llamada de funciones basadas en IPv6 que utilizan las variables de entorno en varios ficheros de configuración de la interfaz y `/etc/sysconfig/network`.
- `ifup-ipx` — Se usa para configurar una interfaz IPX.
- `ifup-plip` — Se usa para configurar una interfaz PLIP.
- `ifup-plusb` — Se usa para configurar una interfaz USB para conexiones de red.
- `ifdown-post` y `ifup-post` — Contiene comandos que se ejecutan después de que una interfaz particular haya sido activada o desactivada.
- `ifdown-ppp` y `ifup-ppp` — Se usa para activar o desactivar una interfaz PPP mediante el uso de un dispositivo en particular.
- `ifup-routes` — Añade rutas estáticas para un dispositivo en particular como si se activase su interfaz.
- `ifdown-sit` and `ifup-sit` — Contiene llamadas de funciones relacionadas con la activación y desactivación de un túnel IPv6 dentro de una conexión IPv4.
- `ifdown-sl` y `ifup-sl` — Se usa para activar o desactivar una interfaz SLIP.

Tenga en cuenta que si elimina o modifica estos scripts puede provocar varias conexiones de interfaz que pueden funcionar de forma extraña o incluso fallar, debido a que los scripts tienden a apoyarse uno en el otro. Sin embargo, los usuarios avanzados pueden modificar los scripts relacionados con una interfaz específica para hacer que se produzcan pasos adicionales cuando esa interfaz se activa o desactiva.

También puede utilizar el script init `/etc/rc.d/init.d/network` para activar o desactivar todas las interfaces de red configuradas para iniciar en el momento de arranque con el comando:

```
/sbin/service network action
```

donde *`action`* es `start` para inciar las interfaces de red, `stop` para interrumpir las interfaces de red o `restart` para reiniciar las interfaces dered. También puede utilizar el comando `/sbin/service/network status` para visualizar una lista de dispositivos configurados y dispositivos activos en la actualidad.

12.4. Funciones de red

Red Hat Linux utiliza varios ficheros que contienen funciones importantes que se usan de modo diverso para activar o desactivar interfaces. Más que fozar cada fichero de control de interfaz para que contenga las mismas funciones que otros, estas funciones están agrupadas convenientemente juntas en algunos ficheros que se pueden suministrar cuando sean necesarios.

El fichero con las funciones de red más comunes es el `network-functions`, localizado en el directorio `/etc/sysconfig/network-scripts`. Este fichero contiene una variedad de funciones IPv4 comunes útil para muchos scripts de control de interfaz, como por ejemplo el contactar con programas en ejecución que han solicitado información sobre cambios en un estado en interfaces, configuración de nombres del host, encontrar dispositivos de puerta de enlace, ver si un dispositivo en particular está o no activado y añadir una ruta por defecto.

Debido a que las funciones solicitadas por las interfaces IPv6 son diferentes de las interfaces IPv4, existe específicamente un fichero `network-functions-ipv6` para sostener esta información. El soporte IPv6 debe ser habilitado en el kernel para comunicar a través de ese protocolo. Existe una función presente en este fichero que comprueba la presencia de soporte IPv6. Además de las funciones que configuran y borran las rutas IPv6 estáticas, crean y borran túneles, añaden y eliminan direcciones IPv6 para una interfaz y comprueban la existencia de una dirección IPv6 en una interfaz que también puede hallarse en este fichero.

12.5. Recursos adicionales

Puede encontrar más información sobre los scripts de red en los siguientes sitios.

- `/usr/share/doc/initscripts-<version>/sysconfig.txt` — Un manual amplio que estudia las opciones disponibles para los ficheros de configuración, incluidas las opciones IPv6 que no cubre este capítulo.
- `/usr/share/doc/iproute-<version>/ip-cref.ps` — Fichero Postscript™ que contiene mucha información sobre el comando `ip`, que se usa para manipular las tablas de routing, entre otras cosas. Use **ghostview** o **kghostview** para ver este fichero.

Capítulo 13.

Firewalls e `iptables`

Linux contiene utilidades avanzadas para *filtrado de paquetes*, el proceso de controlar los paquetes de red cuando entran, se mueven o salen de su sistema dentro del kernel. Los kernels anteriores al 2.4 trabajaban con `ipchains` para efectuar el filtrado de paquetes y usaban listas de reglas que se aplicaban a los paquetes en cada paso del proceso de filtrado. La presentación del kernel 2.4 trajo consigo `iptables` (también llamado *netfilter*), que es parecido a `ipchains` pero con mejoras en el funcionamiento y en el control disponible a la hora de filtrar paquetes.

Este capítulo se centra en las bases del filtrado esencial de paquetes, define las diferencias entre `ipchains` e `iptables`, explica las diferentes opciones disponibles con comandos `iptables`, y muestra cómo las reglas de filtrado se pueden conservar tras el reinicio del sistema.

Si necesita instrucciones para construir reglas de `iptables` o para configurar un firewall basado en estas reglas, consulte Sección 13.5 para más información.

Advertencia

El mecanismo predeterminado del firewall en la versión 2.4 del kernel puede usar el comando `iptables`, pero no se puede usar si ya se está ejecutando `ipchains`. Si `ipchains` está presente durante el arranque, el kernel avisará que hay un error y no podrá arrancar `iptables`.

Estos errores no afectan la funcionalidad del comando `ipchains`.

13.1. Filtrado de paquetes

El tráfico se mueve a través de una red en *paquetes*. Un paquete de red es una colección de datos en diferentes tamaños y formatos. Para enviar un fichero por red, el ordenador emisor debe en primer lugar partirlo en diferentes paquetes usando las reglas del protocolo de red. Cada uno de estos paquetes contiene una parte pequeña de los datos del fichero. Cuando recibe la transmisión, el ordenador receptor reensambla los paquetes y construye de nuevo el fichero el fichero.

Cada paquete contiene información que le ayuda a navegar por la red y moverse hacia su destino. El paquete puede decirle a los ordenadores a lo largo del camino, así como al ordenador destino, de dónde viene, a dónde va, qué tipo de paquete es, y otras muchas cosas más. La mayoría de los paquetes se diseñan para transportar datos, pero algunos protocolos pueden usar los paquetes de forma especial. El protocolo *Transmission Control Protocol (TCP)*, por ejemplo, utiliza un paquete SYN, que no contiene datos, para iniciar la comunicación entre dos sistemas.

El kernel de Linux contiene la característica interna de filtrado de paquetes, que le permite aceptar algunos de ellos en el sistema mientras que intercepta y para a otros. El filtro de red kernel 2.4 tiene tres *tablas* internas o *listas de reglas*. Son las siguientes:

- `filtro` — ésta es la tabla por defecto para manejar paquetes de red.
- `nat` — ésta tabla se usa para alterar paquetes que crean una nueva conexión.
- `mangle` — Esta tabla se usa tipos específicos de alteración de paquetes.

Cada una de estas tablas tiene un grupo de *cadenas* internas que corresponden a las acciones llevadas a cabo por el filtro de red en el paquete.

Las cadenas internas para la tabla `filtro` son las siguientes:

- *INPUT* — Esta cadena sirve solo para paquetes recibidos por medio de una interfaz de red.
- *OUTPUT* — Esta cadena sirve para paquetes enviados por medio de la misma interfaz de red que recibió los paquetes.
- *FORWARD* — Esta cadena sirve para paquetes recibidos en una interfaz de red y enviados en otra.

Las cadenas internas para la tabla `nat` son las siguientes:

- *PREROUTING* — Esta cadena altera paquetes recibidos por medio de una interfaz de red cuando llegan.
- *OUTPUT* — Esta cadena altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.
- *POSTROUTING* — Esta cadena altera paquetes antes de que sean enviados por medio de una interfaz de red.

Las cadenas internas para la tabla `mangle` son las siguientes:

- *PREROUTING* — Esta cadena altera paquetes recibidos por medio de una interfaz de red antes de que sean dirigidos.
- *OUTPUT* — Esta cadena altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.

Cada paquete de red recibido o enviado de un sistema Linux está sujeto a al menos una tabla.

Un paquete puede que sea verificado contra muchas, muchas reglas dentro de la lista de reglas antes de llegar al final de una cadena. La estructura y propósito de estas reglas puede variar, pero normalmente buscan identificar un paquete que viene de o se dirige a una direccción IP en particular o un conjunto de direcciones al usar un determinado protocolo y servicio de red.

Independientemente de su destino, cuando un paquete cumple una regla en particular en una de las tablas, se asignan a un *objetivo (target)* particular, o una acción a aplicárseles. Si la regla especifica un objetivo ACCEPT para un paquete que la cumpla, el paquete se salta el resto de las verificaciones de la regla y se permite que continúe hacia su destino. Si una regla especifica un objetivo DROP, el paquete "se deja caer", significando esto que no se permite que el paquete acceda al sistema y no se envía ninguna respuesta de vuelta al servidor que envió el paquete. Si una regla especifica un objetivo REJECT, el paquete se deja caer, pero se envía un mensaje de error al emisor.

Cada cadena tiene una política ACCEPT, DROP, o REJECT sobre el paquete, o si no, puede enviarlo al espacio de usuario con QUEUE. Si ninguna de las reglas de la cadena se aplican al paquete, entonces el paquete se trata de acuerdo a la política por defecto de las cadenas.

El comando `iptables` le permite configurar estas listas de reglas, así como configurar nuevas cadenas y tablas para ser usadas en si situación particular.

13.2. Diferencias entre `iptables` e `ipchains`

En un primer momento, `ipchains` e `iptables` parecen ser bastante similares. Ambos métodos de filtrado de paquetes usan cadenas o reglas que operan con el kernel de Linux para decidir no solo qué paquetes se permite entrar o salir, sino también qué hacer con los paquetes que cumplen determinadas reglas. Sin embargo, `iptables` ofrece un método mucho más extensible de filtrado de paquetes, proporcionando al administrador un nivel de control mucho más refinado sin tener que aumentar la complejidad del sistema entero.

Más concretamente, los usuarios que se encuentren cómodos con `ipchains` deberían tener cuidado con las siguientes diferencias significativas entre `ipchains` e `iptables` antes de utilizar `iptables`:

- *Bajo iptables, cada paquete filtrado se procesa únicamente usando las reglas de una cadena, en lugar de hacerse con múltiples.* Por ejemplo, un paquete FORWARD que llega al sistema usando ipchains tendrá que pasar por las cadenas INPUT, FORWARD, y OUTPUT para llegar a su destino. Sin embargo iptables, solo envía paquetes a la cadena INPUT si su destino es el sistema local y tan solo los envía a la cadena OUTPUT si el sistema local es quien genera los paquetes. Por esta razón, deberá estar seguro de situar la regla destinada a interceptar un paquete en particular en la cadena adecuada que será la que vea el paquete.

  La principal ventaja es que tendrá un control más refinado sobre la disposición de cada paquete. Si está intentando bloquear el acceso a un sitio web en particular, ahora es posible bloquear los intentos de acceso desde clientes que están en máquinas que utilicen nuestro servidor como pasarela (gateway). Una regla OUTPUT que deniegue el acceso no prevendrá más el acceso a las máquinas que utilicen nuestro servidor como pasarela.
- *El objetivo DENY ha sido cambiado por DROP.* En ipchains, los paquetes que cumplían una regla en una cadena podían ser redirigidos a un objetivo DENY, que dejaba caer el paquete en silencio. Este objetivo deberá cambiarse a DROP con iptables para obtener el mismo resultado.
- *El orden es importante al poner opciones en una regla de una cadena.* Anteriormente, con ipchains, no era muy importante cómo se ordenasen las opciones de las reglas a la hora de escribirla. El comando iptables es un poco más reticente sobre el lugar que ocupan las diferentes opciones. Por ejemplo, ahora deberemos especificar el puerto origen y destino después del protocolo (ICMP, TCP, or UDP) que vayamos a utilizar en una regla de una cadena.
- *Cuando especificamos las interfaces de red que vamos a usar en una regla, deberemos utilizar solo interfaces de entrada (opción -i) con cadenas INPUT o FORWARD y las de salida (opción -o) con cadenas FORWARD o OUTPUT.* Esto es necesario debido al hecho de que las cadenas OUTPUT no se utilizan más con las interfaces de entrada, y las cadenas INPUT no son vistas por los paquetes que se mueven hacia las interfaces de salida.

Esto no es una lista muy extensa de cambios, dado que iptables es fundamentalmente un filtro de red completamente reescrito. Para obtener más información, consulte el documento *Linux 2.4 Packet Filtering HOWTO* y los códigos fuente que podrá encontrar en la Sección 13.5.

13.3. Opciones usadas en comandos iptables

Las reglas que permiten a los paquetes ser filtrados por el kernel se ponen en ejecución ejecutando el comando iptables. Cuando use el comando iptables, debe especificar las opciones siguientes:

- *Packet Type* — éste dicta qué tipo de paquetes filtra el comando.
- *Packet Source or Destination* — éste dicta qué paquetes filtra el comando basándose en el origen o destino del paquete.
- *Target* — éste dicta qué acción se lleva a cabo en paquetes que cumplen los criterios mencionados anteriormente.

Las opciones usadas con la regla dada iptables deben Estar agrupadas lógicamente, basándose en el propósito y en las condiciones de la regla general, para que la regla sea válida.

13.3.1. Tablas

Un aspecto muy potente de iptables es que se pueden utilizar múltiples tablas para decidir el destino de un paquete en particular, dependiendo del tipo de paquete que se esté monitorizando y de qué es lo que se va a hacer con el paquete. Gracias a la naturaleza extensible de iptables se pueden crear tablas especializadas que se almacenarán en el directorio /etc/modules/<*kernel-version*>/kernel/net/ipv4/netfilter para objetivos específicos. Piense que iptables es

capaz de ejecutar múltiples conjuntos de reglas ipchains en las cadenas definidas, en las que cada conjunto cumple un rol específico.

La tabla por defecto, llamada filter, contiene las cadenas estándard por defecto para INPUT, OUTPUT, y FORWARD. Esto es parecido a las cadenas estándar que se utilizan con ipchains. Además, por defecto, iptables también incluye dos tablas adicionales que realizan tareas de filtrado específico de paquetes. La tabla nat se puede utilizar para modificar las direcciones de origen y destino grabadas en un paquetes, y la tabla mangle permite alterar los paquetes de forma especializada.

Cada tabla contiene cadenas por defecto que realizan las tareas necesarias basándose en el objetivo de la tabla, pero se pueden configurar fácilmente nuevas cadenas en el resto de las tablas.

13.3.2. Estructura

Muchos comandos iptables tienen la siguiente estructura:

```
iptables [-t <table-name>] <command> <chain-name> <parameter-1> \
         <option-1> <parameter-n> <option-n>
```

En este ejemplo, la opción <table-name> permite al usuario seleccionar una tabla diferente de la tabla filter por defecto que se usa con el comando. La opción <command> es el centro del comando, dictando cuál es la acción específica a realizar, como pueda ser añadir o borrar una regla de una cadena particular, que es lo que se especifica en la opción <chain-name> . Tras <chain-name> se encuentras los pares de parámetros y opciones que realmente definen la forma en la que la regla funcionará y qué pasará cuando un paquete cumpla una regla.

Cuando miramos a la estructura de un comando iptables, es importante recordar que, al contrario que la mayoría de los comandos, la longitud y complejidad de un comando iptables puede cambiar en función de su propósito. Un comando simple para borrar una regla de una cadena puede ser muy corto, mientras que un comando diseñado para filtrar paquetes de una subred particular usando un conjunto de parámetros específicos y opciones puede ser mucho más largo. Al crear comandos iptables puede ser de ayuda reconocer que algunos parámetros y opciones pueden crear la necesidad de utilizar otros parámetros y opciones para especificar algo de los requisitos de la opción anterior. Para construir una regla válida, esto deberá continuar hasta que todos los parámetros y opciones que requieran otro conjunto de opciones hayan sido satisfechos.

Teclee iptables -h para ver una lista detallada de la estructura de los comandos iptables.

13.3.3. Comandos

Los comandos le dicen a iptables que realice una tarea específica. Solamente un comando se permite por cada cadena de comandos iptables. Excepto el comando de ayuda, todos los comandos se escriben en mayúsculas.

Los comandos de iptables son los siguientes:

- -A — Añade la regla iptables al final de la cadena especificada. Este es el comando utilizado para simplemente añadir una regla cuando el orden de las reglas en la cadena no importa.
- -C — Verifica una regla en particular antes de añadirla en la cadena especificada por el usuario. Este comando puede ser de ayuda para construir reglas iptables complejas pidiéndole que introduzca parámetros y opciones adicionales.
- -D — Borra una regla de una cadena en particular por número (como el 5 para la quinta regla de una cadena). Puede también teclear la regla entera e iptables borrará la regla en la cadena que corresponda.

- `-E` — Renombra una cadena definida por el usuario. Esto no afecta a la estructura de la tabla. Tan solo le evita el problema de borrar la cadena, creándola bajo un nuevo nombre, y reconfigurando todas las reglas de dicha cadena.
- `-F` — Libera la cadena seleccionada, que borra cada regla de la cadena. Si no se especifica ninguna cadena, este comando libera cada regla de cada cadena,
- `-h` — Proporciona una lista de estructuras de comandos útiles, así como una resumen rápido de parámetros de comandos y opciones.
- `-I` — Inserta una regla en una cadena en un punto determinado. Asigne un número a la regla a insertar e `iptables` lo pondrá allí. Si no especifica ningún número, `iptables` posicionará su comando al principio de la lista de reglas.

Atención

Tenga cuidado con qué opción (`-A` o `-I`) está usando al añadir una regla. El orden de las reglas puede ser muy importante cuando esté determinando si se aplica una regla u otra a un paquete en particular. Asegúrese al añadir una regla al principio o al final de la cadena de que no afecta a otras reglas de la misma cadena.

- `-L` — Lista todas las reglas de la cadena especificada tras el comando. Para ver una lista de todas las cadenas en la tabla `filter` por defecto. La sintaxis siguiente deberá utilizarse para ver todas la lsita de todas las reglas de una cadena específica en una tabla en particular:
  `iptables -L <chain-name> -t <table-name>`

  Opciones más potentes para el comando `-L`, que proporcionan números a las reglas y permiten más descripciones en las reglas, así como otros, se pueden ver en la Sección 13.3.7.
- `-N` — Crea una nueva cadena con un nombre especificado por el usuario.
- `-P` — Configura la política por defecto para una cadena en particular de tal forma que cuando los paquetes atravieses la cadena completa sin cumplir ninguna regla, serán enviados a un objetivo en particular, como puedan ser ACCEPT o DROP.
- `-R` — Reemplaza una regla en una cadena en particular. Deberá utilizar un número de regla detrás del nombre de la cadena para reemplazar esta cadena. La primera regla de una cadena se refiere a la regla número `1`.
- `-X` — Borra una cadena especificada por el usuario. No se permite borrar ninguna de las cadenas predefinidas para cualquier tabla.
- `-Z` — Pone ceros en los contadores de byte y de paquete en todas las cadenas de una tabla en particular.

13.3.4. Parámetros

Una vez que se hayan especificado algunos comandos de `iptables` , incluyendo aquellos para crear, añadir, borrar, insertar, o reemplazar reglas de una cadena en particular, se necesitan parámetros para comenzar la construcción de la regla de filtrado de paquetes.

- `-c` Resetea los contadores de una regla en particular. Este parámetro acepta las opciones `PKTS` y `BYTES` para especificar qué contador hay que resetear.
- `-d` Configura el nombre de la máquina destino, dirección IP o red de un paquete que cumplirá la regla. Cuando se especifique una red, puede utilizar dos métodos diferentes para describir la máscara de red, como `192.168.0.0/255.255.255.0` o `192.168.0.0/24`.
- `-f` Aplica esta regla solo a los paquetes fragmentados.

  Usando la opción `!` después de este parámetros, únicamente los paquetes no fragmentados se tendrán en cuenta.

- `-i` Configura las interfaces de entrada de red, como `eth0` o `ppp0`, para ser usadas por una regla en partículas. Con `iptables`, este parámetro opcional solo debería de ser usado por las cadenas INPUT y FORWARD cuando se utilice junto con la tabla `filter` y la cadena PREROUTING con las tablas `nat` y `mangle`.

  Este parámetro proporciona varias opciones útiles que pueden ser usadas antes de especificar el nombre de una interfaz:

  - `!` — Dice a este parámetro que no concuerde, queriendo decir esto que las interfaces especificadas se excluirán de esta regla.
  - `+` — Caracter comodín usado para hacer coincidir todas las interfaces que concuerden con una cadena en particular. Por ejemplo, el parámetro `-i eth+` aplicará esta regla a todas las interfaces Ethernet de su sistema excluyendo cualquier otro tipo de interfaces, como pueda ser la `ppp0`.

  Si el parámetro `-i` se utiliza sin especificar ninguna interfaz, todas las interfaces estarán afectadas por la regla.

- `-j` Dice a `iptables` que salte a un objetivo en particular cuando un paquete cumple una regla en particular. Los objetivos válidos que se usarán tras la opción `-j` incluyen opciones estándard, `ACCEPT`, `DROP`, `QUEUE`, y `RETURN`, así como opciones extendidas que están disponibles a través de módulos que se cargan por defectos con el paquete RPM de `iptables` de Red Hat Linux, como `LOG`, `MARK`, y `REJECT`, así como otras. Mire la página del manual de `iptables` para obtener más información sobre este y otros muchos objetivos, incluyendo reglas de ejemplo que los utilizan, así como objetivos que pueden ser usados sólamente en una tabla en particular.

  En lugar de especificar la acción objetivo, puede también dirigir un paquete que cumpla la regla hacia una cadena definida por el usuario fuera de la cadena actual. Esto le permitirá aplicar otras reglas contra este paquete, y filtrarlo mejor con respecto a otros criterios.

  Si no especifica ningún objetivo, el paquete se mueve hacia atrás en la regla sin llevar a cabo ninguna acción. A pesar de todo, el contador para esta regla se sigue incrementando en uno, a partir del momento en el que el paquete se adecua a la regla especificada.

- `-o` Configura la interfaz de red de salida para una regla en particular, y solo puede ser usada con las cadenas OUTPUT y FORWARD en la tabla `filter` y la cadena POSTROUTING en las tablas `nat` y `mangle`. Estas opciones de los parámetros son los mismos que para los de la interfaz de red de entrada (opción `-i`).
- `-p` Configura el protocolo IP para la regla, que puede ser `icmp`, `tcp`, `udp`, o `all`(todos), para usar cualquier protocolo. Además, se pueden usar otros protocolos menos usados de los que aparecen en `/etc/protocols`. Si esta opción se omite al crear una regla, la opción `all` es la que se selecciona por defecto.
- `-s` Configura el origen de un paquete en particularm usando la misma sintaxis que en el parámetro de destino (opción `-d`).

13.3.5. Opciones de identificación de paquetes

Los diferentes protocolos de red proporcionan opciones especializadas de conconrdancia que pueden ser configurados de forma específica para identificar un paquete en particular usando dicho protocolo. Por supuesto el protocolo deberá ser especificado en un primer momento en el comando `iptables`, como con la opción `-p tcp <nombre-protocolo>`, para hacer que las opciones de dicho protocolo estén disponibles.

13.3.5.1. Protocolo TCP

Estas opciones de identificación están disponibles en el protocolo TCP (opción `-p tcp`):

- `--dport` Configura el puerto de destino para el paquete. Puede utilizar o bien un nombre de servicio de red (como `www` o `smtp`), un número de puerto, o bien un rango de números de puertos para configurar esta opción. Para ver los nombres o alias de los servicios de red y los números de puertos que usan mire el fichero `/etc/services`. Puede usar la opción `--destination-port` para especificar esta opción de identificación de paquete.

  Para especificar un rango de números de puertos separe los dos números de puertos con dos puntos (`:`), como en `-p tcp --dport 3000:3200`. El rango válido más grande es `0:65535`.

  También puede usar el carácter de punto de exclamación (`!`) como flag tras la opción `--dport` para decirle a `iptables` que seleccione los paquetes que *no* usen ese servicio o puerto.
- `--sport` Configura el puerto de origen del paquete, usando las mismas opciones que `--dport`. También puede usar `--source-port` para especificar esta opción.
- `--syn` Provoca que todos los paquetes designados de TCP, comunmente llamados *paquetes SYN*, cumplan esta regla. Cualquier paquete que esté llevando un payload de datos no será tocado. Si se sitúa un punto de exclamación (`!`) como flag tras la opción `--syn` se provoca que todos los paquetes no-SYN sean seleccionados.
- `--tcp-flags` Permite que los paquetes TCP con conjuntos de bits específicos, o flags, sean seleccionados para una regla. La opción de selección `--tcp-flags` acepta dos parámetros, que son los flags para los diferentes bits ordenados en una lista separada por comas. El primer parámetro es la máscara, que configura los flags que serán examinados en el paquete. El segundo parámetro se refiere a los flags que se deben configurar en el paquete para ser seleccionado. Los flags posibles son `ACK`, `FIN`, `PSH`, `RST`, `SYN`, y `URG`. Adicionalmete, se pueden usar `ALL` y `NONE` para seleccionar todos los flags o ninguno de ellos.

  Por ejemplo, una regla `iptables` que contiene `-p tcp --tcp-flags ACK,FIN,SYN SYN` tan solo seleccionará los paquetes TCP que tengan el flag SYN activo y los flags ACK y FIN sin activar.

  Como en otras opciones, al usar el punto de exclamación (`!`) tras `--tcp-flags` invierte el efecto de la opción, de tal forma que los flags del parámetro no tendrán que estar presentes para poder ser seleccionados.
- `--tcp-option` Intenta seleccionar con opciones específicas de TCP que pueden estar activas en un paquete en particular. Esta opción se puede revertir con el punto de exclamación (`!`).

13.3.5.2. Protocolo UDP

Estas opciones de selección están disponibles para el protocolo UDP (`-p udp`):

- `--dport` Especifica el puerto destino del paquete UDP usando el nombre del servicio, el número del puerto, o un rango de puertos. La opción de selección de paquetes `--destination-port` se puede utilizar en lugar de `--dport`. Mire la opción `--dport` en la Sección 13.3.5.1 para ver diferentes formas de utilizar esta opción.
- `--sport` Especifica el puerto origen del paquete UDPm usando el nombre del servicio número de puerto, o rango de puertos. La opción `--source-port` puede ser usada en lugar de `--sport`. Mire la opción en `--dport` en la Sección 13.3.5.1 para ver diferentes formas de utilizar esta opción.

13.3.5.3. Protocolo ICMP

Los paquetes que usan el protocolo de control de mensajes de internet (Internet Control Message Protocol, ICMP) pueden ser seleccionados usando la siguiente opción cuando se especifique `-p icmp`:

- `--icmp-type` Selecciona el nombre o el número del tipo ICMP que concuerde con la regla. Se puede obtener una lista de nombres válidos ICMP tecleando el comando `iptables -p icmp -h`.

13.3.5.4. Módulos con opciones de selección adicionales

Las opciones de selección adicionales, que no son específicas de ningún protocolo en particularm están también disponibles a través de módulos que se cargan cuando el comando `iptables` los necesite. Para usar una de estas opciones deberá cargar el módulo por su nombre incluyendo `-m <nombre-modulo>` en el comando `iptables` que crea la regla.

Un gran número de módulos, cada uno de ellos con sus diferentes opciones de selección de paquetes están disponibles por defecto. También es posible crear sus propios módulos que proporcionen funcionalidades de selección adicionales, puede que para requisitos específicos de su red. Existen muchos módulos, pero tan solo los más populares serán vistos aquí.

El módulo `limit` le permite poner un límite en el número de paquetes que podrán ser seleccionados por una regla en particular. Esto es especialmente beneficioso cuando se usa la regla de logging ya que hace que el flujo de paquetes seleccionados no llene nuestros ficheros log con mensajes repetitivos ni utilice demasiados recursos del sistema.

- `--limit` — Configura el número de coincidencias en un intervalo de tiempo, especificado con un número y un modificador de tiempo ordenados en el formato `<número>/<tiempo>`. Por ejemplo, si usamos `--limit 5/hour` solo dejareños que una regla sea efectiva cinco veces a la hora,

  Si no se utiliza ningún número ni modificador de tiempo, se asume el siguiente valor por defecto: `3/hour`.

- `--limit-burst` — Configura un límite en el número de paquetes capaces de cumplir una regla en un determinado tiempo. Esta opción deberá ser usada junto con la opción `--limit`, y acepta un número para configurar el intervalo de tiempo (threshold).

  Si no se especifica ningún número, tan solo cinco paquetes serán capaces inicialmente de cumplir la regla.

El módulo `state`, aue utiliza la opción `--state`, puede seleccionar un paquete con los siguientes estados de conexión particulares:

- `ESTABLISHED` El paquete seleccionado se asocia con otros paquetes en una conexión establecida.
- `INVALID` El paquete seleccionado no puede ser asociado a una conexión conocida.
- `NEW` El paquete seleccionado o bien está creando una nueva conexión o bien forma parte de una conexión de dos caminos que antes no había sido vista.
- `RELATED` El paquete seleccionado está iniciando una nueva conexión en algún punto de la conexión existente.

Estos estados de conexión se pueden utilizar en combinación con otros separándolos mediante comas como en `-m state --state INVALID,NEW`.

Para seleccionar una dirección MAC hardware de un dispositivo Ethernet en particularm utilice el módulo `mac`, que acepta `--mac-source` con una dirección MAC como opción. Para excluir una dirección MAC de una regla, ponga un punto de exclamación (`!`) tras la opción `--mac-source`.

Para ver otras opciones disponibles a través de módulos, mire la página del manual de `iptables`.

13.3.6. Opciones del objetivo

Una vez que un paquete cumple una regla en particular, la regla puede dirigir el paquete a un número de objetivos (destinos) diferentes que decidirán cuál será su destino y, posiblemente, las acciones adicionales que se tomarán, como el guardar un registro de lo que está ocurriendo. Adicionalmente, cada cadena tiene un objetivo por defecto que será el que se utilice si ninguna de las reglas disponibles

en dicha cadena se pueden aplicar a dicho paquete, o si ninguna de las reglas que se aplican al mismo especifican un objetivo concreto.

Existen pocos objetivos standard disponibles para decidir qué ocurrirá con el paquete:

- *<user-defined-chain>* — El nombre de una cadena que ya ha sido creada y definida con anterioridad junto con esta tabla con reglas que serán verificadas contra este paquete, además de cualquier otra regla en otras cadenas que se deban verificar contra este paquete. Este tipo de objetivo resulta útil para escrutinar un paquete antes de decidir qué ocurrirá con él o guardar información sobre el paquete.
- `ACCEPT` — Permite que el paquete se mueva hacia su destino (o hacia otra cadena, si no ha sido configurado ningún destino ha sido configurado para seguir a esta cadena).
- `DROP` — Deja caer el paquete al suelo. El sistema que envió el paquete no es informado del fallo. El paquete simplemente se borra de la regla que está verificando la cadena y se descarta.
- `QUEUE` — El paquete se pone en una cola para ser manejado por una aplicación en el espacio de usuario.
- `RETURN` — Para la verificación del paquete contra las reglas de la cadena actual. Si el paquete con un destino `RETURN` cumple una regla de una cadena llamada desde otra cadena, el paquete es devuelto a la primera cadena para retomar la verificación de la regla allí donde se dejó. Si la regla `RETURN` se utiliza en una cadena predefinida, y el paquete no puede moverse hacia la cadena anterior, el objetivo por defecto de la cadena actual decide qué acción llevar a cabo.

Además de estos objetivos standard, se pueden usar otros más con extensiones llamadas *módulos de objetivos* (target modules), que trabajan de forma similar a como los hacían los módulos de las opciones de selección. Para obtener más información sobre estos módulos, mire en la Sección 13.3.5.4.

Existen varios módulos extendidos de objetivos, la mayoría de los cuales tan solo se aplicarán a tablas o situaciones específicas. Un par de estos módulos de los más populares e incluidos por defecto en Red Hat Linux serían:

- `LOG` Guarda un registro de todos los paquetes que cumplen esta regla. Como estos paquetes son monitorizados por el kernel, el fichero `/etc/syslog.conf` determina dónde se escribirán esas entradas en el fichero de registro (log). Por defecto, se sitúan en el fichero `/var/log/messages`.

  Se pueden usar varias opciones tras el objetivo `LOG` para especificar la manera en la que tendrá lugar el registro:

  - `--log-level` Configura un nivel de prioridad al evento de registro del sistema. Se puede encontrar una lista de los eventos del sistema en la página del manual de `syslog.conf`, y sus nombres se pueden usar como opciones tras la opción `--log-level`.
  - `--log-ip-options` Cualquier opción en la cabecera de un paquete IP se guarda en el registro.
  - `--log-prefix` Pone una cadena de texto antes de la línea de registro cuando ésta sea escrita. Acepta hasta 29 caracteres tras la opción `--log-prefix`. Esto puede ser útil para escribir filtros del registro del sistema para ser usados conjuntamente junto con el registro de paquetes.
  - `--log-tcp-options` Cualquier opción en la cabecera de un paquete TCP se guarda en el registro.
  - `--log-tcp-sequence` Escribe le número de secuencia TCP del paquete en el registro del sistema.

- `REJECT` Envía un paquete de error de vuelta al sistema que envió el paquete, y lo deja caer (DROP). Este objetivo puede ser útil si queremos notificar al sistema que envió el paquete del problema.

  El objetivo `REJECT` acepta una opción `--reject-with <type>` que permite que información más detallada sea enviada junto con el paquete de error. El mensaje `port-unreachable` es el

error <type> que se envía por defecto cuando no se utiliza junto con otra opción. Para obtener una lista completa de todas las opciones <type> que se pueden utilizar, vea la página del manual de iptables.

Podrá encontrar otras extensiones de objetivos incluyendo algunas muy útiles con masquerading usando la tabla nat o con alteración de paquetes usando la tabla mangle, en la página del manual de iptables.

13.3.7. Opciones de listado

El comando de listado por defecto, iptables -L, proporciona una visión básica de las cadenas actuales de la tabla de filtros por defecto. . Existen opciones adicionales que proporcionan más información y la ordenan de diferentes formas:

- -v Muestra la salida por pantalla, como el número de paquetes y bytes que cada cadena ha visto, el número de paquetes y bytes que cada regla ha encontrado, y qué interfaces se aplican a una regla en particular.
- -x Expande los números en sus valores exactos. En un sistema ocupado, el número de paquetes y bytes vistos por una cadena en concreto o por una regla puede estar abreviado usando K (miles), M (millones), y G (billones) detrás del número. Esta opción fuerza a que se muestre el número completo.
- -n Muestra las direcciones IP y los números de puertos en formato numérico, en lugar de utilizar el nombre del servidor y la red tal y como se hace por defecto.
- --line-numbers Proporciona una lista de cada cadena junto con su orden numérico en la cadena. Esta opción puede ser útil cuando esté intentando borrar una regla específica en una cadena, o localizar dónde insertar una regla en una cadena.

13.4. Guardar información de iptables

Las reglas creadas con el comando iptables se almacenan solamente en RAM. Si tiene que reiniciar su sistema tras haber configurado reglas de iptables, éstas se perderán. Si quiere que determinadas reglas de filtro de red tengan efecto en cualquier momento que inicie su sistema, necesita guardarlas en el fichero /etc/sysconfig/iptables.

Para hacer esto teclee el comando /sbin/service iptables save como usuario root. Esto hace que el script de inicio de iptables ejecute el programa /sbin/iptables-save y escriba la configuración actual de iptables en el fichero /etc/sysconfig/iptables. Este fichero debería ser de solo lectura para el usuario root, para que las reglas de filtrado de paquetes no sean visibles por el resto de los usuarios.

La próxima vez que se inicie el sistema, el script de inicio de iptables volverá a aplicar las reglas guardadas en /etc/sysconfig/iptables usando el comando /sbin/iptables-restore.

Mientras que siempre es una buena idea el verificar cada nueva regla de iptables antes de que se escriba en el fichero /etc/sysconfig/iptables, es posible copiar las reglas de iptables en este fichero a partir de otra versión del sistema de este fichero. Esto le permitirá distribuir rápidamente conjuntos de reglas iptables a diferentes máquinas.

Importante

Si distribuye el fichero /etc/sysconfig/iptables a otras máquinas, debe escribir /sbin/service iptables restart para que las nuevas reglas tengan efecto.

13.5. Recursos adicionales

Vea las fuentes a continuación descritas para mayor información sobre el filtrado de paquetes con el comando `iptables`.

13.5.1. Documentación instalada

- La página del manual de `iptables` contiene una descripción detallada de los diversos comandos, parámetros y otras opciones que podrán ayudarle para añadir nuevas tablas y construir reglas para las cadenas.

13.5.2. Sitios web útiles

- http://netfilter.samba.org — Contiene información diversa sobre `iptables`, incluyendo las FAQ sobre problemas específicos que le pueden ocurrir así como varias guías de ayuda escritas por Rusty Russell, el mantenedor del cortafuegos IP de Linux. La documentación y los cómo cubren temas como conceptos básicos de red, el filtrado de paquetes en los kernels 2.4, configuración de NAT.
- http://www.linuxnewbie.org/nhf/Security/IPtables_Basics.html — una visión básica y general sobre la forma en la que los paquetes se mueven dentro del kernel de Linux, además de una introducción sobre cómo se construyen comandos `iptables` simples.
- http://www.redhat.com/support/resources/networking/firewall.html — Esta página contiene enlaces actualizados a una gran variedad de recursos para el filtrado de paquetes.

Capítulo 14.

Servidor HTTP de Apache

El producto Apache incluye software desarrollado por la Apache Software Foundation (http://www.apache.org).

El servidor HTTP Apache es un servidor Web de tecnología Open Source sólido y para uso comercial desarrollado por Apache Software Foundation (http://www.apache.org). Red Hat Linux 8.0 incluya la versión 2.0 del Servidor HTTP de Apache version 2.0 así como una serie de módulos de servidor diseñados para mejorar la funcionalidad.

El fichero de configuración predeterminado instalado en el Servidor HTTP de Apache funciona en la mayor parte de los casos. Este capítulo subraya cómo personalizar el fichero de configuración de Servidor HTTP de Apache (`/etc/httpd/conf/httpd.conf`) para las situaciones en las que la configuración predeterminada no satisface sus necesidades.

Advertencia

Si desea utilizar la **>Herramienta de configuración de HTTP** (`redhat-config-httpd`), *no* cambie el fichero de configuración de Servidor HTTP de Apache. La herramienta **Herramienta de configuración de HTTP** regenera este fichero cada vez que se usa.

Si desea más información sobre la **Herramienta de configuración de HTTP**, consulte el capítulo *Configuración del servidor HTTP de Apache en el Manual oficial de personalización de Red Hat Linux*.

14.1. Servidor HTTP de Apache 2.0

Red Hat Linux 8.0 viene con la versión 2.0 del Servidor HTTP de Apache. Existen diferencias importantes entre la versión 2.0 y la versión 1.3 — que venía con las anteriores versiones de Red Hat Linux. Esta sección revisa algunas de las nuevas características de la versión 2.0 del Servidor HTTP de Apache y subraya las principales diferencias. Si necesita migrar una versión 1.3 del fichero de configuación al nuevo formato, consulte la Sección 14.2.

14.1.1. Características de la versión 2.0 del Servidor HTTP de Apache

La versión 2.0 del Servidor HTTP de Apache contiene muchas características nuevas. Entre ellas se encuetran las siguientes:

- *Nuevo Apache API* — El Servidor HTTP de Apache contiene un nuevo grupo de Interfaces para la programación de aplicaciones (APIs) más potente y útil para los módulos.

  Advertencia

  Los módulos creados con la versión 1.3 del Servidor HTTP de Apache no funcionan si no se llevan al nuevo API. Si no está seguro de si se ha llevado un determinado módulo, consulte el mantenedor de paquetes antes de la actualización.

- *Filtrado* — Los módulos parala versión 2.0 del Servidor HTTP de Apache actúan como filtros de contenidos. Consulte la Sección 14.2.4 para mayor información.
- *Soporte IPv6* — La versión 2.0 del Servidor HTTP de Apache soporta la próxima generación de las direcciones IP.

- *Directivas simplificadas* — Se han eliminado una serie de directivas complicadas y otras se han simplificado. Consulte la Sección 14.5 para mayor información.
- *Respuestas a errores en diversos idiomas* — Cuando usa documentos *Server Side Include* (*SSI*), aparece un error personalizabel en diversos idiomas.
- *Soporte a diversos protocolos* — La versión 2.0 de Servidor HTTP de Apache soporta diversos protocolos.

En el siguiente sitio se muestra una lista completa de los cambios relaizados: http://httpd.apache.org/docs-2.0/.

14.1.2. Cambios en los paquetes del Servidor HTTP de Apache 2.0

El paquete Servidor HTTP de Apache tiene otro nombre en esta nueva versión. Además otros paquetes se han eliminado y otros se han introducido en otros paquetes.

La siguiente lista contiene los cambios de los paquetes:

- Los paquetes `apache`, `apache-devel` y `apache-manual` ahora se llaman `httpd`, `httpd-devel` y `httpd-manual` respectivamente.
- El paquete `mod_dav` se ha incorporado al paquete `httpd`.
- Se han eliminado los paquetes `mod_put` y `mod_roaming` ya que su funcionalidad aparece recogida en `mod_dav`.
- Se han eliminado los paquetes `mod_auth_any` y `mod_bandwidth`.
- el número de versión del paquete `mod_ssl` se ha sincronizado con el paquete `httpd`. Esto siginifica que el paquete `mod_ssl` para la versión 2.0 del Servidor HTTP de Apache tiene un número de versión *menor* que el paquete `mod_ssl` de la versión 1.3.

14.1.3. Cambios en el sistema de ficheros de la versión 2.0 del Servidor HTTP de Apache

Cambios del sistema de ficheros cuando se actualiza a la versión 2.0 del Servidor HTTP de Apache:

- *Se ha añadido un nuevo directorio de configuración, `/etc/httpd/conf.d/`.* — Este nuevo directorio de usa para alamacenar ficheros de configuración para los módulos individuales como `mod_ssl`, `mod_perl` y `php`. El servidor carga ficheros de configuración desde esta localozación con la directiva `Include conf.d/*.conf` dentro del fichero de configuración del Servidor HTTP de Apache, `/etc/httpd/conf/httpd.conf`.

  Atención

  Es fundamental que se introduzca esta línea cuando migre una configuración ya existente.

- *Se han trasladado los programas `ab` y `logresolve`* — Estos programas se han trasladado desde el directorio `/usr/sbin/` al directorio `/usr/bin/`. Esto hace que fallen scripts con recorridos absolutos para estos binarios.
- *Se ha sustituido el comando `dbmmanage`.* — El comando `dbmmanage` se ha sustotuido con el comando `htdbm`. Consultr la Sección 14.2.4.4 para mayor información.
- *Se ha cambiado el nombre del fichero de configuración `logrotate`.* — Se le ha dado el nombre de `/etc/logrotate.d/httpd`.

La siguiente sección explica cómo migrar a la versión 2.0.

14.2. Migración de los ficheros de configuración de la versión 1.3 del Servidor HTTP de Apache 1.3

Si ha actualizado el servidor en el que Servidor HTTP de Apache ya se abía instalado, entonces la nueva versión se instalará como `/etc/httpd/conf/httpd.conf.rpmnew` y no se tocará la versión 1.3. Usted elije si migrar a la nueva versión o si usar el fichero ya existente y modificarlo para que se adapte; sin embargo, algunas partes del ficherose han cambiado y lo mejor es llegar a un punto intermedio. Los fichero de configuracióln de almacén para ambas versiones están divided en tres secciones. El objetivo es sugerirle la manera más sencilla.

Si el fichero `httpd.conf` es una versión modificada de la versión por defecto de Red Hat y ha guardado una copia del original, entonces le será fácil invocar el comando `diff` como se muestra a continuación:

```
diff -u httpd.conf.orig httpd.conf | less
```

Este comando subraya los cambios realizados. Si no tiene una copia del fichero original, cójalo del paquete RPM usando los comandos `rpm2cpio` y `cpio`, como en el ejemplo siguiente:

```
rpm2cpio apache-1.3.23-11.i386.rpm | cpio -i --make
```

Finalmente, es útil saber que el Servidor HTTP de Apache tiene un modo de prueba para verificar si hay errores en la configuración. Para ello, escriba el siguiente comando:

```
apachectl configtest
```

14.2.1. Global Environment Configuration

La sección del entorno global del fichero de configuración contiene directivas que afectan a toda el áres que cubre el Servidor HTTP de Apache como por ejemplo el número de peticiones que puede recibir al mismo tiempo y las localizaciones de varios ficheros que usa. Esta sección requiere un gran número de cambios comparado con las otras y por ello se recomienda que base esta sección en el fichero de configuración de la versión 2.0 del Servidor HTTP de Apache y que migre a esta versión.

14.2.1.1. Selección de las interfaces y de los puertos a los que vincularse

Ya no existen las directivas `BindAddress` ni `Port` porque quedan recogidas en la directiva `Listen`.

Si tenía configurado el `Puerto 80` en el fichero de configuración de la versión 1.3, debe cambiarlo a `Escuchar 80`. Si el valor del `Puerto` era *más de 80* tiene que poner el número del puerto según los contenidos de la directiva `ServerName`.

Por ejemplo, el siguiente ejemplo es una directiva de la versión 1.3 del Servidor HTTP de Apache:

```
Port 123
ServerName www.example.com
```

Para migrar a la versión 2.0 use la siguiente estructura:

```
Listen 123
ServerName www.example.com:123
```

Para mayor información, consulte la siguiente documentación en el sitio web de la Apache Software Foundation:

- `http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen`
- `http://httpd.apache.org/docs-2.0/mod/core.html#servername`

14.2.1.2. Reagulación del tráfico de peticiones-respuestas del servidor

En la versión 2.0 del Servidor HTTP de Apache se han creado un grupo de módulos llamados *Módulos de procesos múltiples* que se encargan de aceptar las peticiones y de dar procesos hijo para gestionarlos. A diferencia de otros módulos, Servidor HTTP de Apache solamente puede cargar un módulo del grupo MPM ya que un módulo es responsable de las entrega y de la gestión de peticiones. Hay tres módulos MPM que incluye la versión 2.0: prefork, worker y perchild.

El comprotamiento original del Servidor HTTP de Apache 1.3 se ha convertido en prefork MPM. Actualemente solamente está disponible el MPM prefork en el Red Hat Linux aunque se pondrán a la venta los otros máa adelante.

El MPM prefork de Red Hat Linux acepta las mismas directivas que las de la versión 1.3. Las siguientes directivas tienen que migrar directamente:

- `StartServers`
- `MinSpareServers`
- `MaxSpareServers`
- `MaxClients`
- `MaxRequestsPerChild`

Para mayor información consulte la documentación en el sitio web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mpm.html

14.2.1.3. Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)

Se tienen que realizar muchos cambios por eso se recomienda que para modificar la configuración del Apache 1.3 para pasar a la 2 se copie esta sección del fichero de configuración del Red Hat Linux Servidor HTTP de Apache 2.0.

Importante

Si decide modificar el fichero original, observe qye es fundamental que el fichero `httpd.conf` contenga la siguiente directiva:

```
Include conf.d/*.conf
```

Si se omite esta directiva no funcionarán los módulos de los paquetes RPM (como `mod_perl`, `php` y `mod_ssl`).

Aquellas personas que no deseen copiar esta sección del fichero de configuración de la versión 2.0 del Servidor HTTP de Apache tienen que tener en cuenta lo siguiente:

- La directivas `AddModule` y `ClearModuleList` ya no existen. Se usaban para asegurar que los módulos pudierna ser habilitados correctamente. El Apache 2.0 API permite especificar el orden.
- El orden de las líneas `LoadModule` no es importante.
- Muchos módulos han sido eliminados, renombrados o incorporados a otros módulos.
- Ya no son necesarios las líneas `LoadModule` para los módulos empaquetados en los propios RPMs (`mod_ssl`, `php`, `mod_perl` ya que se pueden encontrar en el directorio `/etc/httpd/conf.d/`.

- Las definiciones HAVE_XXX ya no exsiten.

14.2.1.4. Otros cambios en el entorno global

Se han eliminado las siguientes directivas de la configuración del Servidor HTTP de Apache 2.0:

- *ServerType* — El Servidor HTTP de Apache se puede ejecutar solamente como ServerType por lo que esta directiva es irrelevante.
- *AccessConfig* y *ResourceConfig* — Se hane eliminado estas directivas porque su funcionalidad aparece ya en la directiva Include. Si tiene las directivas AccessConfig y ResourceConfig las tiene que sustituir con las directivas Include.

  Para asegurarse que estos ficheros se lean en el orden de las antiguas directivas, las directivas Include tienen que ponerse al final del fichero httpd.conf, en ResourceConfig que precede a AccessConfig. Si está usando los valores predeterminados tiene que incluirlos explicitamente como conf/srm.conf y conf/access.conf.

14.2.2. Configuración del servidor principal

La sección de la configuración del servidor principal del fichero de configruación configura el servidor principal qu equivale a todas aquellas peticiones que no gestiona el <VirtualHost>. Los valores también incluyen los valores predeterminados para todos los contenedores <VirtualHost> que defina.

Las directivas de esta sección han cambiado ligeramente respecto a las de la versión 1.3. Si la configuración del servidor principal está fuertemente personalizada le será fácil modificar la configuración existente para que se adapte a la versión 2.0 de Apache. Los usuarios con configuraciones poco personalizadas tienen que migrar los cambios al ficheros de configuración de Apache 2.0.

14.2.2.1. Asignaciones UserDir

La directiva UserDir se usa para permitir asignaciones de URLS como http://example.com/~jim/ a subdirectorios dentro del directorio principal del usuario jim, como por ejemplo /home/jim/public_html. Un efecto secundario de esta característica es que un atacante potente puede determinar si un nombre de usuaio está en el sistema, por eso esta directiva ha sido eliminada en la nueva versión.

Para habilitar la directiva UserDir, cambie la directiva al httpd.conf desde:

```
UserDir disable
```

al siguiente:

```
UserDir public_html
```

Para mayor información, consulte la documentación en el sitio de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_userdir.html#userdir

14.2.2.2. Conexión

Se han eliminado las siguintes directivas de conexión:

- `AgentLog`
- `RefererLog`
- `RefererIgnore`

Sin embargo, los logs agent y referrer todavía est´n disponibles en las directivas `CustomLog` y `LogFormat`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog
- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#logformat

14.2.2.3. Índice de directorios

Se ha eliminado la directiva `FancyIndexing`. La funcionalidad se encuentra en `FancyIndexing` *opción* en la directiva `IndexOptions`.

La nueva opción `VersionSort` en la directiva `IndexOptions` ordena los números de versión , por ejemplo `httpd-2.0.6.tar` aparece antes de `httpd-2.0.36.tar` en el ílndice de los directorios. page.

Las directivas predeterminadas `ReadmeName` y `HeaderName` han cambiado el nombre por `README.html` y `HEADER.html`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#indexoptions
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#readmename
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#headername

14.2.2.4. Negociación de contenidos

La directiva `CacheNegotiatedDocs` puede estar en `on` o en `off`. Las instancias existentes de `CacheNegotiatedDocs` tienen que ser sustituidas con `CacheNegotiatedDocs on`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_negotiation.html#cachenegotiateddocs

14.2.2.5. Documentos de error

Para usar un menasje altamente codificado con la directiva `ErrorDocument`, el mensaje tiene que aparecer en un par de dobles comillas en vez de una doble comilla como en la versión 1.3 de Apache.

Para migrar la configuración de `ErrorDocument` a la versión 2.0 del Servidor HTTP de Apache use la siguiente estructura:

```
ErrorDocument 404 "The document was not found"
```

Observe que se han puesto las dobles comillas.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/core.html#errordocument

14.2.3. Configuración de las máquinas virtuales

Los contenidos de los contenedores `<VirtualHost>` se tienen que migrar de la misma manera que en la sección del servidor principal como se describe en Sección 14.2.2.

Importante

Oberve que la configuración de las máquinas virtuales SSL/TLS se han quitado del fichero de configuración del servidor principal al fichero `/etc/httpd/conf.d/ssl.conf`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/vhosts/

14.2.4. Módulos y la versión 2.0 del Servidor HTTP de Apache

En la versión 2.0 del Servidor HTTP de Apache, el sistema de módulos se ha cambiado para permitir que los módulos se encadenen o se combinen en maneras nuevas e interesantes. Los scripts CGI, por ejemplo, pueden generar documentos HTML interpretados por el servidor que luego pueden ser procesados por `mod_include`. Esto abre una gran cantidad de posibilidades en lo que respecta a cómo los módulos pueden combianarse para llevar a cabo una meta determinada.

Es decir, cada petición se sirve con el módulo *gestor* seguido de cero o con módulos *filtro*.

En la versión 1.3, un script PHP lo gestiona el módulo PHP. En la versión 2.0, la petición la gestiona inicialmenta el módulo principal — que sirve ficheros estáticos — y que luego filtra el módulo PHP.

Este documento tiene como objetivo describir el uso y las nuevas características de la versión 2.0 de Apache; sin embargo, el cambio tiene ramificaciones si ha usado `PATH_INFO`, que contiene información del recorrido después del nombre del fichero verdadero, en un documento que se gestiona con un módulo que se usa como filtro. EL módulo principal no entiende por defecto `PATH_INFO` y devuelve la pertición como error `404 Not Found`. Puede usar la directiva `AcceptPathInfo` para que el módulo principal acepte las peticiones con `PATH_INFO`. Ejemplo de esta directiva:

```
AcceptPathInfo on
```

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/core.html#acceptpathinfo
- http://httpd.apache.org/docs-2.0/handler.html
- http://httpd.apache.org/docs-2.0/filter.html

14.2.4.1. El módulo `mod_ssl` Module

La configuración del módulo `mod_ssl` ahora está en el fichero `/etc/httpd/conf.d/ssl.conf`. Para cargar este fichero y hacer que `mod_ssl` funcione, tiene que tener la declaración `Include conf.d/*.conf` en `httpd.conf` como se descubre en Sección 14.2.1.3.

Las directivas `ServerName` en las máquinas virtuales SSL tienen que especificar el número del puerto.

Por ejemplo, este es un ejemplo de la directiva de la versión 1.3 del Servidor HTTP de Apache

```
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.host.name
    ...
</VirtualHost>
```

Para migrar a la versión 2.o, use la siguiente estructura:

```
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.host.name:443
    ...
</VirtualHost>
```

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/vhosts/

14.2.4.2. El módulo `mod_proxy`

Las declaraciones de control del acceos proxy se encuentran ahora en el bloque `<Proxy>` y no en `<Directory proxy:>`.

La funcionalidad de caché del antiguo `mod_proxy` se ha dividido en tres módulos:

- `mod_cache`
- `mod_disk_cache`
- `mod_file_cache`

Estos módulos usan en general la mismas directivas o similares como las versiones anteriores del módulo `mod_proxy`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

14.2.4.3. El módulo mod_include

El módulo mod_include se usa como filtro como se muestra en Sección 14.2.4 y se ha habilitado demanera diferente.

Por ejemplo, la siguiente directiva es de la versión 1.3 del Apache:

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Para migrar a la versión 2.0, use la siguiente estructura:

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

Observe que como anteriormente, la directiva Options +Includes se requiere todavía en la sección <Directory> o en el fichero .htaccess.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_include.html

14.2.4.4. Los módulos mod_auth_dbm y mod_auth_db

La versión 1.3 soportaba dos módulos de autenticación, mod_auth_db y mod_auth_dbm, que usaba las bases de datos Berkeley y las DBM respectivamente. Estos módulos se han combinado en un único módulo que se llama mod_auth_dbm en la versión 2.0 del Servidor HTTP de Apache, que puede acceder a las diferentes bases de datos. Para migrar de la versión 1.3 mod_auth_db, los dficheros de configuración se tienen que ajustar sustituyendo AuthDBUserFile y AuthDBGroupFile con los equivalentes mod_auth_dbm: AuthDBMUserFile y AuthDBMGroupFile. Tambié tiene que añadir la directiva AuthDBMType DB para indicar el fichero de la base de datos que usa

He aquí un ejemplo de la versión 1.3 de Apache del fichero mod_auth_db:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBUserFile /var/www/authdb
  require valid-user
</Location>
```

Para migrar a la versión 2.0, use la siguiente estructura:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBMUserFile /var/www/authdb
  AuthDBMType DB
  require valid-user
</Location>
```

Observe que la directiva AuthDBMUserFile también se puede usar en los ficheros .htaccess.

El script Perl dbmmanage que se usa para manipular el nombre del usuario y las bases de datos de contraseñas, se ha sustituido con htdbm en la versión 2.0 del Servidor HTTP de Apache. El programa htdbm ofrece funcionalidad equivalente y como mod_auth_dbm puede operar el una gran variedad de formatos de bases de datos; la opción -T se puede usar en la línea de comandos para especificar el formato que hay que usar.

Tabla 14-1 muestra cómo migrar de una base de datos DBM a htdbm usando el dbmmanage.

Acción	comando dbmmanage (Apache 1.3)	comando equivalente htdbm command (Apache 2.0)
Añada un usuario a la base de datos (usando la contraseña que se ha dado)	`dbmmanage authdb add username password`	`htdbm -b -TDB authdb username password`
Añada un usuario a la base de datos (le pide la contraseña)	`dbmmanage authdb adduser username`	`htdbm -TDB authdb username`
Elimine el usuario de	`dbmmanage authdb delete username`	`htdbm -x -TDB authdb username`
Haga la lista de los usuarios en la base de datos	`dbmmanage authdb view`	`htdbm -l -TDB authdb`
Verique la contraseña	`dbmmanage authdb check username`	`htdbm -v -TDB authdb username`

Tabla 14-1. Migración del `dbmmanage` al `htdbm`

Las opciones `-m` y `-s` trabajan con `dbmmanage` y `htdbm`, permitiendo el uso de los algortimos MD5 o SHA1 para las contraseñas hashing, respectivamente.

Cuando cree una nueva base de datos con `htdbm`, use la opción `-c`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_auth_dbm.html

14.2.4.5. El módulo `mod_perl`

La configuración del módulo `mod_perl` se ha pasado al fichero `/etc/httpd/conf.d/perl.conf`. Para cargar este fichero, y hacer funcionar `mod_perl`, tiene que tener la declaración `Include conf.d/*.conf` en `httpd.conf` tal y como se describe en Sección 14.2.1.3.

Las ocurrencias del `Apache::` en `httpd.conf` tiene que ser sustituido con `ModPerl::`. Además se ha cambiado el modo en los gestores se graban.

Ejemplo de configuración del módulo `mod_perl` en la versión 1.3:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
</Directory>
```

El equivalente `mod_perl` para la versión 2.0 es:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlModule ModPerl::Registry
    PerlHandler ModPerl::Registry::handler
    Options +ExecCGI
</Directory>
```

La mayor parte de los módulos 1.x del `mod_perl` 1.x funcionan sin modificación con los módulos 2.x del `mod_perl` 2.x. Los módulos XS requieren la recompilación y menos modificaciones Makefile.

14.2.4.6. EL módulo `mod_python`

La configuración del `mod_python;` ha pasado al fichero `/etc/httpd/conf.d/python.conf`. Para cargar este fichero y para que funcione `mod_python;`,tiene que tente la declaración `Include conf.d/*.conf` en `httpd.conf` como se muestra en la Sección 14.2.1.3.

14.2.4.7. PHP

La configuración del PHP ha pasado al fichero `/etc/httpd/conf.d/php.conf`. Para cargar este fichero, tiene que tener la declaración `Include conf.d/*.conf` en `httpd.conf` tal y como se muestra en la Sección 14.2.1.3.

El PHP se usa como filtro y tiene que ser habilitado en una manera diferente. Consulte la Sección 14.2.4 para mayor información.

En la versión 1.3, PHP se llevaba a cabo usando las siguientes directivas:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

En la versión 2.0, se usan las siguientes:

```
<Files *.php>
    SetOutputFilter PHP
    SetInputFilter PHP
</Files>
```

En PHP 4.2.0 y en las versiones sucesivas, el set predeterminado de las variable predefinidas que están disponibles en el objetivo global han cambiado. Ya no se ponen en el objetivo global la entrada individual no las variables del servidor. Este cambio hace que se rompan los scripts. Tiene que invertir al antiguo comportamiento poniendo `register_globals` en `On` en el fichero `/etc/php.ini`.

Para mayor información, consulte los siguientes sitios web:

- http://www.php.net/release_4_1_0.php

14.3. Después de la instalación

Tras haber instalado el paquete `apache` podrá encontrar la documentación sobre el servidor de web Apache instalando el paquete `httpd-manual` y apuntando el navegador de web al sitio http://localhost/manual/ o puede navegar en la documentación de Apache disponible en el sitio http://httpd.apache.org/docs-2.0/.

La documentación del Servidor HTTP de Apache contiene una lista completa con decscripciones detalladas de todas las opciones de configuración. Para ayudarle,este capítulo contiene pequeñas descripciones de las directivas de cofiguración que usa la versión 2.o del HTTPD.

La versión de Apache incluida en Red Hat Linux ofrece la posibilidad de configurar servidores Web seguros con la eficaz función de cifrado SSL de los paquetes**mod_ssl** y **OpenSSL**. Cuando lea el fichero de configuración del servidor de Web, tenga en cuenta que la configuración predeterminada incluye tanto el servidor de web seguro como el no seguro. El servidor seguro se ejecuta como una máquina virtual, que aparece configurada en el fichero `/etc/httpd/conf.d/ssl.conf`. Para más información sobre máquinas virtuales, vea la Sección 14.8.2. Para mayor información sobre cómo configurar un servidor seguro HTTP Apache vea el capítulo *Configuración del servidor serguro Apache* en el *Manual oficial de personalización de Red Hat Linux*.

Nota

No se incluyen extensiones FrontPage porque la licencia Microsoft (TM) prohibe la inclusión de extensiones en productos de otras compañías. Para obtener más información sobre las extensiones de Frontpage, consulte http://www.rtr.com/fpsupport/.

14.4. Arranque y apagado del comando `httpd`

El RPM `httpd` instala el script bourne `/etc/rc.d/init.d` al que se accede con el comando `/sbin/service`.

Para arrancar su servidor, teclee el comando:

```
/sbin/service httpd start
```

Si está ejecutando Servidor HTTP de Apache como servidor seguro, se le pedirá que introduzca la contraseña. Después, su servidor arrancará.

Para apagar su servidor, teclee el comando:

```
/sbin/service httpd stop
```

El comando `reanudar` es una manera más corta para apagar y luego reanudar su servidor. El comando `reanudar` apaga y reanuda el servidor. Se le pedirá su contraseña si su servidor Servidor HTTP de Apache es un servidor seguro. El comando `reanudar` tiene el siguiente aspecto:

```
/sbin/service httpd restart
```

Si ha terminado de modificar alguna cosa en el fichero `httpd.conf`, no necesita apagar y reanudar su servidor.Simplemente, utilice el comando `recargar`. Cuando use el comando `recargar`, no tendrá que teclear su contraseña. Durante las recargas se mantendrá su contraseña pero no ocurrirá cuando apague y arranque el servidor. El comando `recargar` tiene el siguiente aspecto:

```
/sbin/service httpd reload
```

El proceso de ejecución del comando `httpd` no comienza automáticamente cuando se arranca el ordenador. Tendrá que configurar el servicio `httpd` para arrancar en el intervalo de arranque usando el initscript como por ejemplo `/sbin/chkconfig`, **/sbin/ntsysv**, o el programa **Herramienta de configuración de servicios**.

Lea el capítulo *Controlar el acceos a los servicios* en *Manual oficial de personalización de Red Hat Linux* para mayor información sobre estas herramientas.

Nota

Si está usando el servidor Servidor HTTP de Apache como un servidor seguro se le pedirá la contraseña despué de que arranque el ordenador a no ser que haya generado una clave para su servidor seguro sin crear la contraseña de protección.

Para mayor información sobre la configuración del servidor seguro Apache HTTPD lea el capítulo *Configuración del servidor seguro Apache HTTP* en el *Manual oficial de personalización de Red Hat Linux*.

14.5. Directivas de configuración en el fichero `httpd.conf`

El fichero de configuración del servidor Web Apache es `/etc/httpd/conf/httpd.conf`. El fichero `httpd.conf` está bien comentado y es bastante autoexplicativo. Sin embargo, quizás quiera conocer el resto de las opciones de configuración más importantes.

Advertencia

Con la versión 2.0 del Servidor HTTP de Apache, han cambiado muchas opciones de configuración. Si necesita migrar de la versión 1.3 al nuevo formato, consulte la Sección 14.2.

Si necesita configurar Servidor HTTP de Apache sólo tiene que modificar el fichero `httpd.conf` y después recargar o bien apagar y arrancar el proceso del comando `httpd`. Para mayor información consulte la Sección 14.4.

Antes de modificar el fichero `httpd.conf` debe de copiar el fichero original dándole por ejemplo, el nombre `httpd.confold` u otro cualquiera. Si crea una copia de seguridad, podrá recuperar el sistema de posibles errores cometidos antes al editar el nuevo fichero de configuración.

Si comete un error y su servidor de web no funciona correctamente, lo primero que debe realizar es revisar lo que lo que acaba de modificar en `httpd.conf`. Asegúrese de no haber cometido ningún gazapo. Después consulte el fichero de conexión de error (`/var/log/httpd/error_log`). Este puede ser difícil de interpretar, todo depende del nivel de experiencia. Si acaba de tener problemas, de todas formas, las últimas entradas deberían de ayudarle a saber lo que ha pasado.

Las siguientes secciones proporcionan una breve descripción de las directivas incluídas en el fichero `httpd.conf`. Las descripciones no son exhaustivas. Si necesita más información, consulte la documentación de Apache en formato HTML en http://httpd.apache.org/docs-2.0/. Para más información sobre las directivas mod_ssl, consulte la documentación incluída en formato HTML en http://httpd.apache.org/docs-2.0/mod/mod_ssl.html.

14.5.1. `ServerRoot`

El comando `ServerRoot` es el directorio principal donde se encuentran todos los ficheros del servidor. Tanto el servidor seguro como el no seguro utilizan un comando `ServerRoot` del `"/etc/httpd"`.

14.5.2. `LockFile`

El comando `LockFile` configura la ruta al fichero de bloqueo utilizado por el servidor Apache cuando se compila con `USE_FCNTL_SERIALIZED_ACCEPT` o `USE_FLOCK_SERIALIZED_ACCEPT`. No se debería de cambiar el valor predeterminado del comando `LockFile`.

14.5.3. `PidFile`

El comando `PidFile` nombra el fichero en el que el servidor graba su ID de proceso (pid). El Red Hat Linux Advanced Server está configurado para grabar su pid en `/var/run/httpd.pid`.

14.5.4. `ScoreBoardFile`

El comando `ScoreBoardFile` almacena información interna sobre el proceso del servidor que se utiliza para comunicar el proceso padre con los procesos hijos. El Red Hat Linux Advanced Server

utiliza memoria compartida para almacenar el comando `ScoreBoardFile`, el predeterminado de `/etc/httpd/logs/apache_runtime_status` sólo se utiliza si es estrictamente necesario.

14.5.5. `Timeout`

El comando `Timeout` define, en segundos, el tiempo que el servidor esperará para recibir y enviar peticiones durante la comunicación. Específicamente, el comando `Timeout` define cuánto esperará el servidor para recibir peticiones GET, cuánto esperará para recibir paquetes TCP en una petición POST o PUT y cuánto esperará entre una ACK y otra respondiendo a paquetes TCP. El comando `Timeout` está ajustado a 300 segundos, que es el tiempo apropiado para la mayoría de las situaciones.

14.5.6. `KeepAlive`

El comando `KeepAlive` determina si el servidor permitirá varias peticiones de conexión a la vez (es decir, conexiones continuas). `KeepAlive` puede usarse para impedir que un cliente consuma muchos recursos del servidor. El comando `KeepAlive` se establece en `off` por defecto, lo que significa que no se permiten varias conexiones a la vez. Puede definirse en `on` para para que sí sean posibles. En la mayoría de los casos, deseará que Keepalive esté desactivado ya que Apache sólo puede tener un número limitado de procesos hijo y estos procesos dependerán de otros y esperarán a que se establezca una conexión futura desde el el mismo cliente. Si activa Keepalives, también deberá establecer KeepAliveTimeout (consulte Sección 14.5.8) en un valor bajo y controlar el registro de errores (error_log) de los servidores `/var/log/httpd/error_log` para estar advertido si no dispone de suficientes procesos hijo para gestionar las peticiones.

14.5.7. `MaxKeepAliveRequests`

Esta directiva establece el número máximo de peticiones permitidas por cada conexión que se produzca a la vez. El Grupo Apache recomienda un valor alto, lo que mejoraría el rendimiento. El valor predeterminado del comando `MaxKeepAliveRequests` es de `100` que debería bastar en la mayoría de los casos.

14.5.8. `KeepAliveTimeout`

La directiva `KeepAliveTimeout` establece el número de segundos que el servidor esperará a la siguiente petición, tras haber dado servicio a una petición, antes de cerrar la conexión. Una vez recibida la petición, aplica la directiva `Timeout` en su lugar.

14.5.9. `MinSpareServers` y `MaxSpareServers`

El servidor Servidor HTTP de Apache se ;adapta dinámicamente a la carga percibida manteniendo un número apropiado de servidores libres basado en el tráfico. El servidor comprueba el número de servidores que esperan peticiones y elimina algunos si el número es más alto que `MaxSpareServers` o crea algunos si el número de servidores es menor que `MinSpareServers`.

El valor predeterminado de `MinSpareServers` es `5` y el de `MaxSpareServers` es `20`. Estos valores predeterminados son suficientes en la mayoría de los casos. El número de `MinSpareServers` no debería de ser elevado ya que creará una gran carga incluso cuando el tráfico fuese bajo.

14.5.10. `StartServers`

`StartServers` establece cuántos procesos serán creados al arrancar. Ya que el servidor Web crea y elimina dinámicamente servidores según el tráfico, no se necesitará cambiar este parámetro. El servidor está configurado para arrancar ocho procesos al arrancar.

14.5.11. `MaxClients`

El comando `MaxClients` establece un límite al total de los procesos del servidor (es decir, clientes conectados simultáneamente) que se ejecutan a la vez. Debe mantener el comando `MaxClients` a un valor alto (el valor por defecto es 150), porque no se permitirán nuevas conexiones una vez que se alcance el número máximo de clientes simultáneamente conectados. El valor del comando `MaxClients` no puede superar el 256 sin que se haya recompilado Apache. La principal razón de tener el parámetro `MaxClients` es evitar que un servidor errático vuelva inestable al sistema operativo.

14.5.12. `MaxRequestsPerChild`

El comando `MaxRequestsPerChild` establece el número máximo de peticiones que cada proceso hijo procesa antes de morir. La principal razón para tener el comando `MaxRequestsPerChild` es evitar que procesos de larga vida pierdan memoria. El valor predeterminado de `MaxRequestsPerChild` para el servidor es de `100`.

14.5.13. `Listen`

El comando `Listen` establece los puertos en los que Red Hat Linux Advanced Server acepta las peticiones entrantes. Red Hat Linux Advanced Server está configurado para el escuchar en el puerto 80 para comunicaciones no seguras y (en máquinas virtuales que define el servidor seguro) en el puerto 443 para comunicaciones seguras.

Para puertos por debajo de 1024, el comando `httpd` deberá ser ejecutado como root. Para el puerto 1024 y superiores, el comando `httpd` puede ser ejecutado como si se fuera un usuario cualquiera.

El comando `Listen` también se puede usar para especificar direcciones IP específicas en las cuales aceptará conexiones el servidor.

14.5.14. `Include`

`Include` permite que se incluyan otros ficheros de configuración en el tiempo de ejecución.

El recorrido de estos ficheros puede ser absoluto o relativo con respecto al comando `ServerRoot`.

Importante

Para que el servidor use módulos de paquetes individuales, como `mod_ssl`, `mod_perl`, y `php`, la siguiente directiva tiene que estar en `Section 1: Global Environment` del `http.conf`:

```
Include conf.d/*.conf
```

14.5.15. LoadModule

El comando LoadModule se usa para cargar módulos Dynamic Shared Object(DSO). Para más información sobre el soprte de los DSOs de Apache y cómo usar la directiva LoadModule, lea la Sección 14.7. Nótese que el orden de los módulos ya no es importante en la versión 2.0. Consulte la Sección 14.2.1.3 para mayor información sobre el soporte del DSO de la versión 2.0 del HTTPD;.

14.5.16. IfDefine

Las etiquetas <IfDefine> y </IfDefine> rodean a directivas de configuración que son aplicadas si el test aplicado a la etiqueta <IfDefine> resulta verdadero; las directivas no se tienen en cuenta si el test es falso.

Dicho test aplicado a la etiqueta <IfDefine> es un nombre de un parámetro (p.e., HAVE_PERL). Si el parámetro está definido,es decir, si se da como argumento al comando de arranque del servidor, entonces el test es verdadero. En este caso, cuando se arranca el Red Hat Linux Advanced Server el test es verdadero y se aplican las directivas contenidas en las etiquetas IfDefine.

Por defecto, las etiquetas <IfDefine HAVE_SSL> rodean las etiquetas de la máquina virtual del servidor seguro. Las etiquetas <IfDefine HAVE_SSL> también rodean a las directivas LoadModule y a las AddModule para ssl_module.

14.5.17. ExtendedStatus

La directiva ExtendedStatus controla si Apache genera información de estado básico (off) o detallada (on), cuando se llama al gestor server-status. Se llama al gestor Server-status utilizando la etiqueta Location; Para mayor información sobre cómo llamar al server-status consulte la Sección 14.5.65

14.5.18. User

La directiva User establece el userid usado por el servidor para responder a peticiones. El valor de User determina el acceso al servidor. Cualquier fichero al que no pueda acceder este usuario será también inaccesible al visitante de la web. El comando predeterminado para User es apache.

User debería sólo tener privilegios de tal manera que sólo puediera acceder a ficheros que se supone que todo el mundo puede ver. El comando User también es dueño del cualquier proceso CGI que arranque el servidor.Al comando User no se le debería permitir ejecutar ningún código que no esté pensado para responder peticiones HTTP.

Nota

Por razones de seguridad, Servidor HTTP de Apache rechazará la ejecución como User root. Usar root para User creará grandes problemas de seguridad para el servidor de Web.

El proceso httpd padre se ejecuta como root duranteoperaciones normales, pero pasa al usuario apache inmediatamente. El servidor debe arrancar como root porque necesita un puerto por debajo de 1024 (El puerto predeterminado para comunicaciones seguras es 443; el puerto por defecto para comunicaciones no seguras es el puerto 80). Los puertos por debajo de 1024 están reservados para el sistema, así que sólo se pueden usar si se es root. Una vez que el servidor se ha conectado al puerto, pasa el proceso a User antes de aceptar peticiones.

14.5.19. Group

El comando Group es similar a User. Group establece el grupo en el que el servidor responde a las peticiones. El valor predeterminado del comando Group es apache.

14.5.20. ServerAdmin

ServerAdmin debería ser la dirección de correo del administrador del Red Hat Linux Advanced Server. Esta dirección de correo aparecerá en los mensajes de error generados por el servidor para páginas web,de tal manera que los usuarios pueden comunicar errores enviando correo al administrador. El comando ServerAdmin ya se encuentra en la dirección root@localhost.

Una forma buena y típica de configurar ServerAdmin es situarlo en la dirección webmaster@your_domain.com. Después cree un alias del webmaster para la persona responsable del servidor en /etc/aliases. Finalmente, ejecute /usr/bin/newaliases para añadir el nuevo alias.

14.5.21. ServerName

El comando ServerName puede usarse para establecer el nombre de la máquina del servidor diferente al nombre real de máquina como por ejemplo, usar www.your_domain.com aunque el nombre real del servidor sea foo.your_domain.com. Nótese que ServerName debe ser un nombre "Domain Name Service" (DNS) válido que se tenga derecho a usar (no basta con inventar uno). Por ejemplo:

```
ServerName www.your_domain.com:80
```

Si se especifica ServerName, hay que asegurarse de incluir la pareja nombre-dirección IP en el fichero /etc/hosts.

14.5.22. DocumentRoot

DocumentRootes el directorio que contiene la mayoría de los ficheros HTML que se entregarán en respuesta a peticiones. El directorio predeterminado DocumentRoot para servidores seguros y no seguros es /var/www/html. Por ejemplo, el servidor puede recibir una petición para el siguiente documento:

```
http://your_domain/foo.html
```

El servidor buscará el fichero en el siguiente directorio por defecto:

```
/var/www/html/foo.html
```

Si se quiere cambiar DocumentRoot para que no lo compartan los servidores seguros y no seguros, vea la Sección 14.8.

14.5.23. Directory

Las etiquetas <Directory /path/to/directory> y </Directory> se usan para agrupar directivas de configuración que sólo se aplican a ese directorio y sus subdirectorios. Cualquier directiva aplicable a un directorio puede usarse en las etiquetas <Directory>. Las etiquetas <File> pueden aplicarse de la misma forma a un fichero específico.

Por defecto,se aplican parámetros muy restrictivos al directorio raíz, utilizando `Options` (vea la Sección 14.5.24) y `AllowOverride` (vea la Sección 14.5.25). Con esta configuración, cualquier directorio del sistema que necesite valores más permisivos ha de ser configurado explícitamente.

La utilización de las etiquetas `Location`, permite al comando `DocumentRoot` (referido a `"/"`) tener parámetros menos rígidos para que el servidor sirva las peticiones HTTP.

El directorio `cgi-bin` está configurado para permitir la ejecución de scripts CGI, con la opción `ExecCGI`. Si se necesita ejecutar un script CGI en cualquier otro directorio, habrá que configurar `ExecCGI` para ese directorio. Por ejemplo, si `cgi-bin` es `/var/www/cgi-bin`, pero se quiere ejecutar scripts CGI desde `/home/my_cgi_directory`, añadirá una directiva `ExecCGI` a un par de directivas `Directory` como las siguientes al fichero `httpd.conf`:

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Para permitir la ejecución de scripts CGI en `/home/my_cgi_directory`, habrá que llevar a cabo pasos extra aparte de configurar `ExecCGI`. También necesitará anular el comentario de la directiva `AddHandler` para identificar ficheros con extensión `.cgi` como scripts CGI. Vea la Sección 14.5.59 para saber cómo configurar el comando `AddHandler`. El valor de los permisos para scripts CGI y el recorrido entero a los scripts, debe ser de 0755.

14.5.24. `Options`

La directiva `Options` controla características del servidor que están disponibles en un directorio en particular. Por ejemplo, en los parámetros restrictivos especificados para el directorio raíz, el comando `Options` sólo permite `FollowSymLinks`. No hay características permitidas, salvo que el servidor pueda seguir enlaces simbólicos en el directorio raíz.

Por defecto, en el directorio `DocumentRoot`, `Options` está configurado para incluir los comandos `Indexes`, `Includes` y `FollowSymLinks`. `Indexes` permite al servidor generar un listado de un directorio si no se especifica el `DirectoryIndex` (`index.html, etc.`). `Includes` implica que se permiten inclusiones en el servidor y el comando `FollowSymLinks` permite al servidor seguir enlaces simbólicos en ese directorio.

También se tienen que incluir declaraciones del comando `Options` para los directorios que estén dentro de directivas de máquinas virtuales, si se quiere que éstas reconozcan esas `Options`.

Por ejemplo, la inclusión en el servidor está activada en el directorio `/var/www/html` en la línea `Options Includes` dentro de la sección `Location "/"`. Sin embargo, si se quiere que una máquina virtual reconozca que se permite realizar la inclusión desde el servidor en `/var/www/html`, habrá que incluir una sección como la siguiente desde dentro de las etiquetas de las máqinas virtuales:

```
<Directory /var/www/html>
Options Includes
</Directory>
```

14.5.25. `AllowOverride`

`AllowOverride` establece qué directivas `Options` puede obviar un fichero `.htaccess`. Por defecto, tanto el directorio raíz como `DocumentRoot` están configurados para no permitir la prevalencia de `.htaccess`.

14.5.26. `Order`

`Order` simplemente controla el orden en que `allow` y `deny` se evaluan. El servidor está configurado para evaluar `Allow` antes que `deny` para el directorio `DocumentRoot`.

14.5.27. `Allow`

`Allow` especifica qué peticionario puede acceder un directorio dado. El peticionario puede ser `all`, un nombre de dominio, una dirección IP, una dirección IP parcial, un par de máscaras de red, etc. El directorio `DocumentRoot` está configurado para permitir peticiones de `all` (cualquiera).

14.5.28. `Deny`

`Deny` funciona como `allow`, pero especifica a quién se niega el acceso. `DocumentRoot` no está configurado para `rechazar` peticiones de nadie.

14.5.29. `UserDir`

`UserDir` es el nombre del subdirectorio dentro del directorio de cada usuario dónde estarán los ficheros HTML que serán servidos por el servidor de Web.

Por defecto, el subdirectorio es `public_html`. Por ejemplo, el servidor podría recibir la siguiente petición:

`http://your_domain/~username/foo.html`

El servidor buscaría el fichero:

`/home/username/public_html/foo.html`

En el ejemplo, `/home/username` es el directorio del usuario (nótese que la ruta predeterminada a los directorios de los usuarios puede variar entre sistemas).

Hay que asegurarse que los permisos de los directorios de usuario sean correctos. El valor de los permisos deben ser de 0711. Los bits de lectura (r) y ejecución (x) deben estar activados en el directorio del usuario `public_html` (0755 valdrá). El valor de los permisos con que se servirán los ficheros desde `public_html` debe ser 0644 por lo menos.

14.5.30. `DirectoryIndex`

`DirectoryIndex` es la página por defecto que entrega el servidor cuando hay una petición de índice de un directorio especificado con una barra (/) al final del nombre del directorio.

Por ejemplo, cuando un usuario pide la página http://*`your_domain`*/*`this_directory`*/, recibe la página `DirectoryIndex` si existe, o un listado generado por el servidor. El valor por defecto para `DirectoryIndex` es `index.html`, `index.htm` `index.shtml` e `index.cgi`. El servidor intentará encontrar cualquiera de estos cuatro, y entregará el primero que encuentre. Si no encuentra ninguno y si `Options Indexes` se encuentra en el directorio, el servidor generará un listado, en formato HTML, de los subdirectorios y ficheros del directorio.

14.5.31. AccessFileName

AccessFileName denomina el fichero que el servidor utilizará para controlar el acceso en cada directorio. Por defecto, el servidor utilizará .htaccess, si existe, para controlar el acceso en cada directorio.

Justo tras AccessFileName,el comando Files controla el acceso a cualquier fichero que empiece con .ht. Estas directivas niegan acceso a todo tipo de fichero .htaccess (u otros ficheros que empiecen .ht) por razones de seguridad.

14.5.32. CacheNegotiatedDocs

Por defecto, el Red Hat Linux Advanced Server requiere a los "proxies" que no hagan caché de los documentos que se negocian en base al contenido (pueden cambiar en el tiempo o según los datos del peticionario). Si se anula el comentario del comando CacheNegotiatedDocs, se desactiva la función y los "proxies" podrán hacer caché de los documentos.

14.5.33. UseCanonicalName

UseCanonicalName ya aparece en on. El comando UseCanonicalName permite que los URLs contengan sus propias referencias utilizando los comandos ServerName y Port. Cuando el servidor se refiere a si mismo en respuesta a peticiones de clientes, usa este URL. Si el UseCanonicalName está en off, el servidor utilizará el valor que vino en la petición del cliente para referirse a si mismo.

14.5.34. TypesConfig

TypesConfig denomina el fichero que establece la lista predeterminada de mapeado de tipos MIME (extensiones de ficheros a tipos de contenido). El fichero predeterminado TypesConfig es /etc/mime.types. En vez de modificar el /etc/mime.types, se recomienda añadir mapeados de tipos MIMEs con AddType.

Para obtener más información sobre el comando AddType, consulte Sección 14.5.58.

14.5.35. DefaultType

DefaultType establece el contenido por defecto que el servidor utilizará para documentos cuyos tipos MIME no puedan ser determinados. El servidor predispone el texto para cualquier fichero con un tipo de contenido indeterminado.

14.5.36. IfModule

<IfModule> y </IfModule> envuelven a directivas que son condicionales. Las directivas contenidas dentro de IfModule son procesadas si se cumple una de las dos condiciones. Las directivas son procesadas si el módulo contenido en la etiqueta <IfModule> está cargado en el servidor Apache. O, si una "!" (exclamación) aparece antes del nombre; las directivas son procesadas sólo si el módulo en la etiqueta <IfModule> *no* está compilado.

El fichero mod_mime_magic.c está incluído en IfModule. El módulo mod_mime_magic puede compararse al comando UNIX file, que examina los primeros bytes de un fichero, y usa "números mágicos" y otros trucos para decidir el tipo MIME del fichero.

Si el módulo mod_mime_magic está compilado en Apache, estas etiquetas IfModule le dicen al módulo mod_mime_magic module donde está el fichero de los trucos: share/magic en este caso.

El módulo mod_mime_magic module no está compilado por defecto. Si se quier usar, vea la Sección 14.7, para saber cómo añadir módulos al servidor.

14.5.37. HostnameLookups

`HostnameLookups` puede aparecer en `on` o en `off` o en `doble`. Si el servidor permite la directiva `HostnameLookups` (poniéndolo en `on`), el servidor resolverá automáticamente la dirección IP de cada conexión que pida un documento del servidor. Resolver la dirección IP implica que el servidor hará una o más conexiones al DNS para averiguar qué nombre de máquina se corresponde con una dirección IP. Si lo pone en `doble`, su servidor lleva a cabo la resolución doble DNS. En otras palabras, después de un lookup inverso, se lleva a cabo un lookup directo. Finalmente, una del as direcciones IP en el lookup directo tiene que coincidir con la dirección del primero lookup inverso.

Generalmente, debería dejarse `HostnameLookups` en `off` porque las peticiones de DNS añanden carga al servidor y pueden ralentizarlo. Si el servidor tiene carga, los efectos de `HostnameLookups` serán considerables.

`HostnameLookups` influye también en Internet en general. Cada conexión individual provoca una sobrecarga en el servidor. Por ello, por beneficio del servidor y de Internet en general, debería dejarse `HostnameLookups` en `off`.

Para ver los nombres de host de los ficheros .log, puede ejecutar una de las muchas herramientas de análisis de ficheros .log que realizan consultas de DNS de una forma más eficaz y ejecuciones en grupo para cambiar los ficheros .log.

14.5.38. ErrorLog

`ErrorLog` nombra el fichero donde se guardan los errores del servidor. Como viene indicado, el fichero de error del servidor es `/var/log/httpd/error_log`.

El log de errores es un buen sitio para ver si el servidor genera errores y no se desconoce como ha sucedido.

14.5.39. LogLevel

`LogLevel` establece cómo serán de abundantes los logs de error. Los niveles de error del `LogLevel` (de menor a mayor) son `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` or `debug`. El `LogLevel` del Red Hat Linux Advanced Server está en `warn` (nivel medio).

14.5.40. LogFormat

`LogFormat` pone el formato para los mensajes en el log de acceso. El comando `LogFormat` real que se use dependerá de los parámetros definidos en la directiva `CustomLog` (consulte la Sección 14.5.41).

14.5.41. CustomLog

`CustomLog` identifica el log y el formato de log. La configuración por defecto de `CustomLog` del Red Hat Linux Advanced Server, define el log en el que se guardan los accesos al servidor `/var/log/httpd/access_log`. Habrá que saber la localización de este fichero si se quieren generar estadísticas de rendimiento del servidor.

`CustomLog` pone el formato combinado para el fichero. El formato común de log es de la siguiente forma:

```
remotehost rfc931 authuser [date] "request" status bytes  referer
user-agent
```

remotehost

El nombre de la máquina: Si el nombre no está disponible en el DNS, o sí `HostnameLookups` está en `Off`, entonces *remotehost* será la dirección IP de la máquina remota.

rfc931

No utilizado: Se verá un - en el log en su lugar.

authuser

Si se requirió la autenticación, este es el usuario con el que el usuario se identificó. Generalmente, no se usa, así que se verá un - en su lugar.

[date]

Fecha y hora de la petición.

"request"

Cadena de texto de la petición según vino del cliente.

status

Código de estado HTTP que se devolvió al cliente.

bytes

Tamaño del documento.

herramienta de referencias

Puede proporcionar la dirección URL de la página Web vinculada a la petición actual.

agente de usuario

Proporciona el nombre del navegador o cliente que realiza la petición.

14.5.42. `ServerSignature`

El comando `ServerSignature` añade una línea que contiene la versión del servidor Apache y el `ServerName` de la máquina a los documentos generados por el servidor (p.ej, mensajes de error devueltos a clientes). `ServerSignature` ya aparece en `on`. Se puede cambiar a `off` para no añadir nada, o se puede cambiar a `EMail`. `EMail` añadirá una etiqueta HTML `mailto:ServerAdmin` a la línea de firma.

14.5.43. `Alias`

El comando `Alias` permite que haya directorios fuera del `DocumentRoot` a los que puede acceder el servidor. Cualquier URL que termine en un alias será automáticamente traducido por el recorrido del alias. Por defecto, ya existe un alias configurado. El servidor puede acceder al directorio `icons` pero el directorio no está en `DocumentRoot`. `icons`, un alias, está en `/var/www/icons/`, y no en `/var/www/html/icons/`.

14.5.44. `ScriptAlias`

El comando `ScriptAlias` define dónde pueden encontrarse los scripts CGI (u otros scripts). Normalmente, no se ponen los scripts CGI dentro de `DocumentRoot`. Si los scripts CGI se encontrasen en `DocumentRoot`, podrían, potencialmente, ser considerados como documentos de texto. Incluso si no preocupa que la gente vea (y use) los scripts CGI, mostrar cómo funcionan crea oportunidades a la gente sin escrúpulos que quiera explotar dichos agujeros en el script, y puede crear un agujero de seguridad en el servidor. Por defecto, el directorio `cgi-bin` es un `ScriptAlias` de `/cgi-bin/`, y se encuentra situado `/var/www/cgi-bin/`.

El directorio `/var/www/cgi-bin` tiene activada la directiva `Options ExecCGI`, lo que implica que se permite la ejecución de scripts CGI en el directorio.

Vea la Sección 14.5.59 y la Sección 14.5.23 para saber cómo ejecutar scripts CGI en otros directorios aparte de `cgi-bin`.

14.5.45. `Redirect`

Cuando se cambia una página de sitio, el comando `Redirect` se puede usar para pasar del viejo URL al nuevo URL. El formato es como sigue:

```
Redirect /path/foo.html
http://new_domain/path/foo.html
```

Así que si se recibe una petición HTTP para un página que solía estar en http://*your_domain*/*path*/foo.html, el servidor devolverá el nuevo URL (http://*new_domain*/*path*/foo.html) al cliente, que tratará de coger el documento desde el nuevo URL.

Para aplicar un redireccionamiento más avanzado puede usar el módulo `mod_rewrite` que se incluye con el servidor.

14.5.46. `IndexOptions`

El comando `IndexOptions` controla la apariencia de los listados generados por el servidor, al añadir iconos y texto descriptivo, etc. Si `Options Indexes` aparece como en (véase la Sección 14.5.24), el servidor podrá generar el listado de un directorio al recibir una petición HTTP como la que sigue:

http://*your_domain*/*this_directory*/

Primero el servidor busca en el directorio un fichero de los de la lista de `DirectoryIndex` (p.ej., `index.html`). Si el servidor no encuentra ninguno de los ficheros, genera un listado del directorio en HTML. Se puede modificar la apariencia del listado utilizando ciertas directivas en `httpd.conf`, entre las que se encuentra `IndexOptions`.

La configuración predeterminada activa es `FancyIndexing`. Si se activa `FancyIndexing`, al hacer click en la cabecera de las columnas del listado, el listado se ordena según esa columna. Otro click en la misma cabecera cambiará el orden de ascendente a descendente y viceversa. `FancyIndexing` también muestra distintos iconos para distintos ficheros, según la extensión. Si se usa la directiva `AddDescription` y se activa `FancyIndexing`, se añade una pequeña descripción para el fichero en el listado generado.

`IndexOptions` tiene otros parámetros que pueden activarse para controlar la apariencia de los listados. Los parámetros incluyen `IconHeight` e `IconWidth`, para hacer que el servidor incluya etiquetas `HEIGHT` y `WIDTH` para los iconos; el comando `IconsAreLinks`, hace que los iconos formen parte del enlace HTML junto con el nombre del fichero, y otros.

14.5.47. AddIconByEncoding

Esta directiva denomina qué iconos se mostrarán con los ficheros según su codificación MIME, en los listados de directorio. Por ejemplo, por defecto, el servidor muestra el icono `compressed.gif` junto a ficheros con codificación MIME x-compress y x-gzip en los listados de directorio.

14.5.48. AddIconByType

Esta directiva denomina qué iconos se mostrarán con los ficheros según su codificación MIME, en los listados del directorio. Por ejemplo, por defecto, el servidor muestra el icono `text.gif` junto a ficheros con tipo MIME "text" en los listados del directorio.

14.5.49. AddIcon

`AddIcon` dice al servidor qué icono mostrar en los listados del directorio para ciertos tipos de ficheros según la extensión. Por ejemplo, el servidor muestra el icono `binary.gif` para ficheros con extensiones `.bin` o `.exe`.

14.5.50. DefaultIcon

El comando `DefaultIcon` nombra el icono de los listados del directorio que recibirán los ficheros sin un icono específico. El fichero de imagen predeterminado para esos ficheros `unknown.gif` es `DefaultIcon`.

14.5.51. AddDescription

Se puede usar `AddDescription` para mostrar descripciones específicas de ficheross en los listados de los directorios (habrá que activar también el `FancyIndexing` como una `IndexOptions`). Puede aplicarse a ficheros individuales, expresiones de nombre o extensiones para especificar los ficheros a los que aplicar esta directiva. Por ejemplo, podría usarse lo siguiente:

```
AddDescription "A file that ends in .ni" .ni
```

En los listados del directorio, todos los ficheros con extensión `.ni` tendrán la descripción `Un fichero` que termina en `.ni` tras el nombre. Nótese que necesita activarse el `FancyIndexing`.

14.5.52. ReadmeName

La directiva `ReadmeName` determina el fichero (si existe dentro del directorio) que se adjuntará a los listados de los directorios. El servidor intentará primero incluirlo como documento HTML y luego como texto. El valor predeterminado de `ReadmeName` es `README`.

14.5.53. HeaderName

La directiva `HeaderName` dicta el fichero (si existe dentro del directorio) que se antepondrá al comienzo de los listados de los directorios. Al igual que con `ReadmeName`, el servidor intentará incluirlo como documento HTML si es posible, o como texto.

14.5.54. `IndexIgnore`

El comando `IndexIgnore` lista las extensiones, los nombres de los ficheros parciales, las expresiones regulares o los nombres completos. El servidor no incluirá los ficheros que encajen en estos patrones en los listados de directorios.

14.5.55. `AddEncoding`

El comando `AddEncoding` dice qué extensiones especifican un tipo particular de codificación. `AddEncoding` se puede usar para decirle a los navegadores (no a todos) que descompriman ciertos ficheros mientras los descargan.

14.5.56. `AddLanguage`

La directiva `AddLanguage` asocia extensiones a contenidos específicos de idiomas. Esta directiva es útil para la negociación de contenidos, cuando el servidor devuelve uno de entre varios documentos según las preferencias de idiomas del cliente.

14.5.57. `LanguagePriority`

La directiva `LanguagePriority` permite dar la prioridad a ciertos ficheros en distintos idiomas, que entrarán en vigor si el cliente no especifica la preferencia de idioma.

14.5.58. `AddType`

Use la directiva `AddType` para definir parejas de tipos MIME y sus extensiones. Por ejemplo, si usa el PHP4, el servidor está usando `AddType` para que se reconozcan ficheros con extensiones PHP (`.php4`, `.php3`, `.phtml` `.php`) como tipos MIME PHP.

La siguiente línea `AddType` permite al servidor reconocer las extensiones `.shtml` (para la inclusión en el servidor):

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Se necesitará la línea de arriba dentro de las etiquetas de máquina virtual para cuando se permita la inclusión desde el servidor.

14.5.59. `AddHandler`

La directiva `AddHandler` mapea y amplia gestores específicos. Por ejemplo, el gestor `cgi-script` puede usarse para hacer que la extensión `.cgi` automáticamente sea manejada como un script CGI. Esto funciona, incluso para ficheros fuera de `ScriptAlias`, si se siguen las instrucciones dadas.

Hay una línea `AddHandler` CGI en `httpd.conf` como la siguiente:

```
AddHandler cgi-script .cgi
```

Habrá que anular el comentario de la línea. Así Apache ejecutará como scripts CGI los ficheros que terminen en `.cgi`, incluso si están fuera de `ScriptAlias`, que por defecto se encuentra en el directorio `/cgi-bin/` en `/var/www/cgi-bin/`.

También habrá que activar `ExecCGI` como `Options` para cualquier directorio que contenga scripts CGI. Vea Sección 14.5.23 para más información sobre cómo configurar `ExecCGI` para un directorio. Además, habrá que asegurarse que los permisos sean los adecuados para los scripts CGI y los subdirectorios que contengan scripts. Los scripts CGI y todo el recorrido que conduce a ellos deben tener un valor de 0755.

Habrá que añadir la misma línea `AddHandler` a la configuración de `VirtualHost`, si se usan máquinas virtuales y se quiere que se reconozcan los scripts CGI fuera de `ScriptAlias`.

El servidor también usa `AddHandler` para procesar mapas de imágenes en HTML.

14.5.60. `Action`

La directiva `Action` permite especificar un par de tipos de contenido MIME y un script CGI, de tal forma que cuando se pida un fichero de este tipo, se ejecute un script en particular.

14.5.61. `MetaDir`

`MetaDir` especifica el nombre del directorio donde el servidor debería buscar los ficheros que contengan información meta (cabeceras extra de HTTP) que se deba incluir al entregar los documentos.

14.5.62. `MetaSuffix`

`MetaSuffix` especifica el sufijo para los ficheros que contienen información meta (cabeceras extra de HTTP), que estarán en el directorio `MetaDir`.

14.5.63. `ErrorDocument`

Por defecto, en caso de error, el servidor muestra un mensaje de error (generalmente críptico) para el cliente. En vez de usar esta opción ya predeterminada, puede usarse `ErrorDocument` para devolver un mensaje de error personalizado o redireccionar al cliente a un URL local o remoto. `ErrorDocument` simplemente asocia un código de respuesta HTTP con un mensaje o un URL que se devolverá al cliente.

Importante

Tiene que incluir el mensaje de erroe en un par de comillas para que sea válido.

14.5.64. `BrowserMatch`

La directiva `BrowserMatch` permite al servidor definir variables de entorno y/o tomar acciones según sea el campo de cabecera User-Agent, que identifica al cliente. Por defecto, el servidor usa `BrowserMatch` para denegar la conexión a navegadores con problemas conocidos y para desactivar "keepalives" y vaciados de cabecera de HTTP para navegadores con problemas de esas características.

14.5.65. `Location`

Las etiquetas `<Location>` y `</Location>` permiten controlar el acceso específico a cada URL.

Si se quiere que las conexiones desde dentro del mismo dominio tengan acceso a los informes de estado, se debe anular el comentario de la siguiente sección de directivas:

```
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Hay que poner el segundo nivel del nombre de dominio en vez de `.your_domain.com`.

Si se quiere dar informes de configuración del servidor (incluyendo módulos instalados y directivas de configuración) o peticiones desde dentro del dominio, habrá que anular el comentario de las siguientes líneas:

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Hay, por supuesto, que rellenar `.your_domain.com`.

14.5.66. `ProxyRequests`

Si se anula el comentario de la directiva `IfModule` alrededor del `ProxyRequests`, el servidor Apache también funcionará como proxy. También habrá que cargar el módulo `mod_proxy`. Para más información sobre cómo cargar módulos, vea la Sección 14.7.

14.5.67. `ProxyVia`

La directiva `ProxyVia` controla si se envía HTTP Via: junto con peticiones o respuestas que vayan vía el servidor proxy Apache. Via: header mostrará el nombre de la máquina si `ProxyVia` aparece en `On`, el nombre de máquina y la versión de Apache para `Full`, y cualquier línea Via: se enviará sin cambiar si está ProxyVia está en `Off`, y las líneas Via: serán eliminadas si está en `Block`.

14.5.68. Directivas de caché

Hay varias directivas de caché en las etiquetas de proxy `IfModule` mencionadas antes. Si se usa la funcionalidad proxy y se quiere habilitar el caché proxy, habrá que anular el comentario de las directivas según se describe. Los valores predeterminados de las directivas de caché deberían bastar para la mayoría de las configuraciones.

`CacheRoot` pone el nombre del directorio que contiene ficheros de caché. El valor predeterminado de `CacheRoot` es `/var/cache/httpd`.

`CacheSize` establece cuánto espacio puede usar el caché, en KB. El valor predeterminado de `CacheSize` es `5` KB.

`CacheGcInterval` establece el número de horas. Tras ese número se borrarán los ficheros de caché si ocupan más de lo permitido por `CacheSize`. El valor por defecto de `CacheGcInterval` es cuatro horas.

Los documentos HTML en caché se guardarán (sin una recarga desde el servidor de origen) durante el número máximo de horas establecido por `CacheMaxExpire`. El valor predeterminado es `24` horas.

`CacheLastModifiedFactor` afecta a la fecha de caducidad para documentos que no venían con caducidad desde el servidor de origen. El valor predeterminado de `CacheLastModifiedFactor` es `0.1`, lo que significa que la caducidad del documento será un décimo del tiempo total desde que se modificó el documento por última vez.

`>CacheDefaultExpire` es la caducidad en horas para documentos recibidos vía protocolos que no soportan la caducidad. El valor predeterminado es de una hora.

Todo documento que provenga de una máquina y/o de un dominio que encaje en `NoCache` no se pondrá en caché. Si conoce máquinas o dominios en los que no se quiera hacer caché de sus documentos, anule el comentario de la directiva `NoCache` e introduzca dominios y nombres aquí.

14.5.69. `NameVirtualHost`

Necesitará usar la directiva `NameVirtualHost` para la dirección IP (y número de puerto si es necesario) de algún nombre de máquinas virtuales que esté estableciendo. La configuración basada en máquinas virtuales se usa para establecer máquinas virtuales para diferentes dominios, pero no tiene (o no usa) diferentes direcciones IP para todos los dominios a los cuales su Web Server sirve documentos

Nota

No puede usar nombres basados en máquinas virtuales con su servidor seguro. Algunos nombres basados en máquinas virtuales que establezca trabajarán sólo con conexiones HTTP no seguras y no con conexiones SSL.

Si está usando nombres basados en máquinas virtuales, comente la directiva `NameVirtualHost` y añada la dirección IP correcta para su servidor después del `NameVirtualHost`. Entonces añada más información sobre los diferentes dominios usando el comando `VirtualMachine` el cual envuelve el `ServerName` para cada máquina virtual, más algunas otras directivas de configuración que son sólo aplicables a la máquina virtual.

14.5.70. `VirtualHost`

`<VirtualHost>` y `</VirtualHost>` envuelven directivas de configuración que se aplican a máquinas virtuales. La mayoría de las directivas de configuración pueden usarse en etiquetas de máquina virtual, y sólo se aplicarán a esa máquina virtual.

Existen varias etiquetas `VirtualHost` que rodean a algunos modelos de directivas de configuración así como de espacios en blanco que tendrá que rellenar con información para configurar la máquina virtual. Consulte la Sección 14.8, para saber más sobre máquinas virtuales.

Nota

Todos los contextos de las máquinas virtuales SSL se han pasado al fichero `/etc/httpd/conf.d/ssl.conf`.

14.5.71. `SetEnvIf`

La directiva de configuración de Apache `SetEnvIf` se puede usar para establecer variables de entorno basadas en las cabeceras de la petición. El fichero `httpd.conf` sirve para desactivar HTTP keepalive y permitir a SSL cerrar las conexiones sin avisar desde el cliente. Este parámetro es necesario para clientes que no cierran bien la conexión SSL.

14.5.72. Directivas de configuración SSL

Se han incluído las directivas SSL en su fichero de servidores `/etc/httpd/conf.d/ssl.conf` para permitir comunicaciones seguras Web usando las directivas SSL.

Para mayor información sobre la configuración del servidor seguro Apache HTTP, vea el capítulo *Configuración del servidor seguro Apache HTTPD* en el *Manual oficial de personalización de Red Hat Linux*.

Nota

No modifique sus directivas SSl a menos que esté completamente seguro de lo que está haciendo. Para la mayoría de los Red Hat Linux Advanced Server, las directivas SSL están configuradas e instaladas apropiadamente.

14.6. Módulos predeterminados

El Servidor HTTP de Apache incluye un número de módulos. Por defecto, los siguientes módulos están instalados y activados con el paquete `httpd` en Red Hat Linux:

```
mod_access
mod_auth
mod_auth_anon
mod_auth_dbm
mod_auth_digest
mod_include
mod_log_config
mod_env
mod_mime_magic
mod_cern_meta
mod_expires
mod_headers
mod_usertrack
mod_unique_id
mod_setenvif
mod_mime
mod_dav
mod_status
mod_autoindex
mod_asis
mod_info
mod_cgi
mod_dav_fs
mod_vhost_alias
mod_negotiation
mod_dir
mod_imap
```

```
mod_actions
mod_speling
mod_userdir
mod_alias
mod_rewrite
```

Además, los siguientes módulos están disponibles si instala paquetes adicionales:

```
mod_auth_mysql
mod_auth_pgsql
mod_perl
mod_python
mod_ssl
php
squirrelmail
```

14.7. Añadir módulos a su servidor

Debido a que Servidor HTTP de Apache 2.0 soporta DSOs, puede fácilmente cargar módulos Apache o compilar sus propios módulos para su Red Hat Linux Advanced Server. DSO significa que se pueden cargar los módulos en tiempo de ejecución. Debido a que los módulos se cargan sólo cuando es necesario no usan la memoria hasta que la necesitan.

El grupo Apache da información completa en http://httpd.apache.org/docs-2.0/dso.html . Después de la instalación del paquete `http-manual` consulte también http://*`your_domain`*/manual/mod/.

Para que el Servidor HTTP de Apache use un módulo dinámicamente compartido, este módulo debe tener una línea `LoadModule` y otra `AddModule` en `httpd.conf`.

Si necesita usar uno de estos módulos no cargados, mire en el fichero `httpd.conf` para ver todos los módulos posibles. Cada uno de estos módulos tiene una línea `LoadModule`. Para ver un ejemplo, la sección `LoadModule` comienza con estas siete líneas:

Un ejemplo de la línea `LoadModule` es el siguiente:

```
LoadModule access_module modules/mod_access.so
```

Si añade o elimina módulos del `http.conf`, tiene que recargar o reanudar Apache, tal y como se indica en Sección 14.4.

Si tiene su propio módulo, puede añadirlo al fichero `httpd.conf` y así se compila y se carga como un DSO. Si quiere llevar a cabo esta operación, necesita instalar el paquete `apache-devel`. Necesita este paquete `apache-devel` porque instala el fichero include, los ficheros cabeceras y el soporte de herramientas APache eXtenSion (APXS). APXS usa los ficheros include y los ficheros cabecera para compilar su módulo y así poder trabajar con Apache.

Si ha escrito su propio módulo o utiliza módulos de terceros, podrá usar APXS para compilar sus módulos fuentes fuera del árbol fuente Apache, sin necesitar ningún indicador del compilador y/o del creador de enlaces. Si necesita más información sobre APXS consulte la documentación en http://httpdapache.org/docs-2.0/dso.html y la página man `apxs`.

Una vez compilados sus módulos usando APXS, situélos dentro de `/usr/lib/httpd`. Entonces su módulo necesita ambas líneas `LoadModule`, `AddModule` en el fichero `httpd.conf`, como se describe para los módulos de Apache. Después en la lista `LoadModule` en el `httpd.conf`, añada una línea para el fichero objeto compartido para el módulo como la siguiente:

```
LoadModule <foo_module> modules/<mod_foo.so>
```

Observe que necesitará cambiar el nombre de <*`foo_module`*> and <*`mod_foo.so`*>. apropiadamente.

Una vez que haya completado los pasos previos, pare y reinicialice su servidor Web como se indica en la Sección 14.4. Si ha hecho todo correctamente, y su módulo está correctamente codificado, su servidor Web encontrará su módulo y lo cargará.

14.8. Utilización de máquinas virtuales

Se puede utilizar la capacidad de las máquinas virtuales de Apache para ejecutar servidores en distintas direcciones IP, diferentes nombres o diferentes puertos en la misma máquina. Si está interesado en utilizar máquinas virtuales,puede encontrar toda la información en la documentación de Apache en el sitio http://www.apache.org/docs-2.0/vhosts/.

Nota

El Red Hat Linux Advanced Server no admite usar máquinas virtuales que estén basadas en el nombre porque el acuerdo SSL (cuando el cliente acepta el certificado SSL del servidor) ocurre antes de la petición HTTP que identifica por el nombre a la máquina virtual apropiada. Si se quieren utilizar este tipo de máquinas virtuales, lo podrá hacer sólo con servidores no seguros.

Las máquinas virtuales se configuran en `httpd.conf`, según se describe en la Sección 14.5. Por favor, lea esta sección antes de empezar a cambiar la configuración de las máquinas virtuales del servidor.

14.8.1. Máquina virtual del Red Hat Linux Advanced Server

La configuración predeterminada de Red Hat Linux Advanced Server se ejecuta en servidores seguros y no seguros. Ambos servidores usan la misma dirección IP y nombre, pero diferentes puertos, y el servidor seguro es una máquina virtual. Esta configuración permite entregar documentos seguros y no seguros de la manera más eficiente posible. La configuración de una transmisisón HTTP segura utiliza muchos recursos y, por ello, podrá ofrecer menos páginas por segundo con un servidor seguro. Tenga en cuenta esto cuando decida qué información va a incluir en el servidor seguro y qué información puede usar en un servidor no seguro.

Las directivas de configuración del servidor seguro están en las etiquetas de la máquina virtual en `/etc/httpd/conf.d/ssl.conf`. Si se necesita cambiar la configuración del servidor seguro, habrá que cambiar las directivas que se encuentran en las etiquetas de la máquina virtual.

Por defecto, los servidores seguros y no seguros comparten el mismo `DocumentRoot`, directiva de configuración especificada en `httpd.conf`. En otras palabras, los servidores buscan en el mismo sitio los ficheros que proporcionan como respuesta a las peticiones. El valor predeterminado de `DocumentRoot` es `conf.d/ssl.conf`.

Para cambiar `DocumentRoot`, de tal forma que no lo compartan el servidor seguro y el no seguro, cambie una de las directivas `DocumentRoot` en `httpd.conf`. La directiva `DocumentRoot` fuera de las etiquetas de la máquina virtual define la directiva `DocumentRoot` para el servidor no seguro. Así mismo la directiva `DocumentRoot` dentro de las etiquetas de la máquina virtual la define para el servidor seguro.

El servidor seguro usa el puerto 443, puerto por defecto para comunicaciones web seguras, mientras que el servidor no seguro usa el puerto 80, el puerto predeterminado para las comunicaciones web. Para evitar que el servidor no seguro acepte conexiones, busque la línea siguiente en `httpd.conf`:

```
Port 80
```

Cambie la línea:

```
Port 443
```

Anule el comentario de la línea `Listen 80`.

14.8.2. Configuración de las máquinas virtuales

Para crear una máquina virtual, habrá que alterar las líneas de la máquina virtual dadas como ejemplo en `httpd.conf`, o crear una sección de máquinas virtuales.

Las líneas wue sirven de ejemplo de una máquina virtual son las siguientes:

```
#<VirtualHost  *>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

Anule el comentario de las líneas (elimínese # al comienzo de cada línea). Añada entonces la información correcta para la máquina y/o máquina virtual a cada línea.

En la primera línea, cambie `ip.address.of.host.some_domain.com` por la dirección IP del servidor. Cambie `ServerName` por un nombre DNS *válido* para la máquina virtual. (En otras palabras, no basta con inventar algo. Pregunte al administrador de red si no sabe cómo conseguir un nombre de dominio válido.)

También habrá que anular el comentario de las líneas `NameVirtualHost` en `httpd.conf`:

```
NameVirtualHost*
```

Anule el comentario de una de las líneas y cambie la dirección IP por la dirección (y puerto si es necesario) para esa máquina virtual.

```
NameVirtualHost 192.168.1.1:80
```

Se pueden poner en las etiquetas otras directivas de configuración para la máquina virtual, según cómo se configure ésta.

Si se configura una máquina virtual para escuchar en un puerto no habitual (80 es el valor predeterminado para comunicaciones no seguras y 443 es el defecto para comunicaciones seguras), habrá que configurar una máquina virtual para el puerto y añadir la directiva `Listen` `httpd.conf`, correspondiente a ese puerto.

Para tener una máquina virtual específica para ese puerto, añada el puerto a la primera línea de la configuración de la máquina virtual. La primera línea debería parecerse a lo siguiente:

```
<VirtualHost ip_address_of_your_server:12331>
```

Esta línea crearía una máquina virtual en el puerto 12331. Sustituya `12331` por el puerto que desea usar en el ejemplo anterior.

En las líneas `Listen` de `httpd.conf`, añada lo siguiente para que el servidor escuche en el puerto 12331:

Hay que rearrancar el servidor para iniciar una nueva máquina virtual. Vea la Sección 14.4 para mayor información sobre cómo arrancar y apagar `httpd`.

Podrá encontrar información mucho más completa sobre cómo crear y configurar máquinas virtuales según el nombre y la dirección IP en la página web en http://www.apache.org/docs-2.0/vhosts/index.html.

14.9. Recursos adicionales

Hay disponible mucha información sobre Apache. Revise estas fuentes de información, especialmente el sitio Web oficial de Apache y el sitio Web de mod_ssl.

14.9.1. Sitios Web útiles

- http://httpd.apache.org — El sitio Web oficial del servidor Web Apache con documentación sobre todas las directivas y módulos por defecto.
- http://www.modssl.org — Sitio Web oficial de mod_ssl.
- http://www.apacheweek.com — Publicación semanal en línea.

14.9.2. Libros relacionados

- *Apache Desktop Reference* by Ralf S. Engelschall; Addison Wesley

  Escrito por un miembro de ASF y autor de mod_ssl,Ralf Engelschall, *Apache Desktop Reference* proporciona una gía de referencia completa sobre el uso de Apache en los procesos de compilación, configuración y ejecución. Este libro también se puede descargar en línea: http://www.apacheref.com/.
- *Professional Apache* by Peter Wainwright; Wrox Press Ltd

  Professional Apache es uno de los muchos libros de la serie de Wrox Press Ltd's "Programmer to Programmer", destinado a usuarios avanzados de Apache y administradores de servidores Web que usan Apache por primera vez.
- *Administering Apache* by Mark Allan Arnold; Osborne Media Group

  Libro destinado a los ISP que desean ofrecer servicios más seguros, Desarrolladores de Web, programadores y administradores de Sistema corporativos.
- *Apache Server Unleashed* by Richard Bowen, et al; SAMS BOOKS

  El libro de Rich Bowen y Ken Coar pretende convertirse en una Fuente enciclopédica de Apache.
- *Apache Pocket Reference* by Andrew Ford, Gigi Estabrook; O'Reilly

  Apache Pocket Reference by Andrew Ford es la última novedad de la serie O'Reilly Pocket Reference.

Capítulo 15.

Correo electrónico

El correo electrónico o email es uno de los servicios de Internet que más se utilizan. Red Hat Linux ofrece varios modos de utilizar el correo electrónico, independientemente de si usted es un usuario de un equipo de sobremesa o un administrador del sistema.

En este capítulo se analizan los protocolos de correo electrónico más conocidos actualmente, así como varios programas diseñados para realizar distintos tipos de tareas relacionadas con el correo electrónico.

15.1. Protocolos

El correo electrónico, al igual que otros servicios de red, utiliza diversos protocolos. Estos protocolos permiten que máquinas distintas, que se ejecutan a menudo en sistemas operativos diferentes y que tienen instalados programas de correo electrónico distintos, se comuniquen entre sí y transfieran correo electrónico para que llegue a los destinatarios adecuados.

Los protocolos que se indican a continuación son los que más se utilizan para transferir correo electrónico de un sistema a otro.

15.1.1. IMAP

El protocolo *IMAP (Internet Message Access Protocol, Protocolo de acceso a mensajes de Internet)* es un método que utilizan las aplicaciones cliente de correo electrónico para obtener acceso a los mensajes almacenados remotamente. Al utilizar el protocolo IMAP, normalmente denominado IMAP4 después de la versión del protocolo en cuestión, los mensajes de correo electrónico se conservan en el servidor de correo remoto, donde el usuario puede leerlos o eliminarlos, además de cambiar el nombre o eliminar los buzones de correo para almacenar correo electrónico.

Además, el protocolo IMAP es totalmente compatible con importantes estándares de mensajes de Internet, como, MIME (Multipurpose Internet Mail Extensions, Extensiones de correo de Internet multipropósito), que permiten recibir ficheros adjuntos. Muchos clientes de correo electrónico que utilizan el protocolo IMAP también se pueden configurar para que se almacene temporalmente en caché una copia de los mensajes localmente, de modo que el usuario puede examinar los mensajes que ha leído anteriormente si no está conectado directamente al servidor IMAP.

IMAP lo utilizan principalmente los usuarios que pueden obtener acceso a su correo desde varias máquinas, como mensajes almacenados en una ubicación central y a los que puede acceder cualquier sistema que utilice una cliente de correo IMAP y una conexión con el servidor IMAP remoto. También los usuarios que se conectan a Internet o a una red privada a través de una conexión de ancho de banda baja utilizan a menudo el protocolo IMAP, puesto que sólo la información de cabecera del correo se obtiene inicialmente. Esto les permite posponer la descarga de mensajes que tienen ficheros adjuntos de gran tamaño hasta el momento en el que no se utilice la banda de ancho limitada. De la misma manera, el usuario puede eliminar el correo electrónico que no le interesa sin tener que ver antes el cuerpo del mensaje, lo cual evita el tener que descargar un mensaje mediante la conexión de red que utilicen.

Los documentos *RFC (Request for Comment, Petición de comentarios)* del protocolo IMAP contienen detalles y especificaciones sobre cómo debe funcionar el protocolo. El documento RFC-1730 define en primer lugar el modo en el que el protocolo IMAP debe utilizar la versión 4, pero RFC-2060 contiene las cuestiones de implantación de IMAP actuales que utilizan muchos servidores IMAP y que se denomina versión IMAP4rev1.

El paquete `imap` de Red Hat Linux permite a los usuarios conectarse al sistema y recibir correo electrónico con el protocolo IMAP. Se admiten conexiones IMAP gracias a la integración de la tecnología SSL (Secure Socket Layer, ÇÇ) en el demonio `imapd`, que permite usar el fichero de certificados `/usr/share/ssl/certs/imapd.pem`. No es necesario utilizar el programa `stunnel` para el cifrado SSL de las conexiones IMAP, aunque no obstante se puede usar. Consulte la Sección 15.6.2 para obtener más información sobre estas dos opciones de cifrado.

También hay disponibles otros clientes y servidores IMAP gratuitos y comerciales, los cuales amplían el protocolo IMAP y proporcionan funciones adicionales. Para obtener una lista completa, visite la dirección URL http://www.imap.org/products/longlist.htm.

15.1.2. POP

El protocolo *POP (Post Office Protocol, Protocolo de oficina de correo)* permite a los clientes de correo electrónico recuperar los mensajes de los servidores remotos y guardarlos en las máquinas locales. La mayoría de los clientes de correo que utilizan el protocolo POP se configuran automáticamente para eliminar el mensaje del servidor de correo después de transferirlo correctamente al sistema del cliente, aunque esto se puede cambiar.

Para establecer una conexión a un servidor POP, el cliente de correo abre una conexión TCP en el puerto 110 del servidor. Cuando la conexión se ha establecido, el servidor POP envía al cliente POP una invitación y después las dos máquinas se envían entre sí otros comandos y respuestas que se especifican en el protocolo. Como parte de esta comunicación, al cliente POP se le pide que se autentifique en lo que se denomina *Estado de autenticación*, donde el nombre de usuario y la contraseña del usuario se envían al servidor POP. Si la autenticación es correcta, el cliente POP pasa al *Estado de transacción*, fase en la que se pueden utilizar los comandos `LIST`, `RETR` y `DELE` para mostrar, descargar y eliminar mensajes del servidor, respectivamente. Los mensajes definidos para su eliminación no se quitan realmente del servidor hasta que el cliente POP envía el comando `QUIT` para terminar la sesión. En ese momento, el servidor POP pasa al *Estado de actualización*, fase en la que se eliminan los mensajes marcados y se limpian todos los recursos restantes de la sesión.

POP es un protocolo mucho más sencillo que IMAP, porque no se tienen que enviar tantos comandos entre el cliente y el servidor. POP también es en cierta medida más conocido, aunque la mayoría de los clientes de correo electrónico pueden utilizar cualquiera de estos protocolos.

La mayoría de los usuarios que utilizan el protocolo POP sólo tienen un sistema y descargan los mensajes en sus máquinas para su almacenamiento. El protocolo POP también funciona adecuadamente si no se utiliza una conexión constante a Internet o a la red que contiene el servidor de correo. El protocolo IMAP se puede configurar también actualmente para almacenar los mensajes localmente de modo que se puedan ver los mensajes mientras no se está conectado a la red.

En varios documentos RFC se proporciona una explicación sobre el protocolo POP, aunque es en el documento RFC-1939 en el que se ofrece una descripción básica del protocolo POP3, la versión actual del protocolo.

También se pueden ejecutar otras versiones del protocolo POP menos utilizadas, como, por ejemplo:

- *APOP* — POP3 con autenticación MDS. En este protocolo, el cliente de correo envía un hash codificado de la contraseña al servidor, en lugar de enviar la contraseña en texto plano.
- *KPOP* — POP3 con autenticación Kerberos. Consulte el Capítulo 10 para obtener más información sobre la autenticación Kerberos.
- *RPOP* — POP3 con autenticación RPOP, que utiliza un identificador de usuario similar a una contraseña para autenticar las peticiones del protocolo POP. No obstante, este identificador o ID no está codificado, de modo que RPOP no es más seguro que el protocolo POP normal.

En Red Hat Linux hay disponibles muchos servidores, clientes y otras aplicaciones POP. Si prefiere utilizar un cliente de correo electrónico gráfico, **Mozilla Mail** es una opción perfecta. Además, con otros programas, como Fetchmail, se puede recuperar el correo electrónico mediante el protocolo POP.

Si utiliza el sistema Red Hat Linux como servidor de correo, el paquete `imap` contiene los demonios POP2 (`ipop2`) y POP3 (`ipop3`) en el directorio `/usr/sbin`.

15.1.3. SMTP

Mientras que los protocolos IMAP y POP permiten que un usuario reciba y lea el correo electrónico, el protocolo*SMTP (Simple Mail Transfer Protocol, Protocolo simple de transferencia de correo)* sirve para enviar correo electrónico. Los mensajes salientes utilizan SMTP para pasar de la máquina del cliente al servidor, lugar desde el que se trasladan hasta el destino final. También dos servidores de correo que intentan transferir entre sí un mensaje utilizan SMTP para comunicarse, incluso si utilizan plataformas totalmente distintas.

SMTP usa el puerto 25 del servidor para comunicarse. Empieza un intercambio SMTP básico con el sistema conectado mediante la emisión del comando `MAIL From: <dirección de correo electrónico>` para iniciar el intercambio. El sistema que recibe el comando responde con un mensaje `250` para informar de que se ha recibido el primer comando. A continuación, el sistema conectado comunica las direcciones de correo electrónico para recibir el mensaje del sistema receptor, seguido de un mensaje con el comando `DATA`. Este mensaje notifica al sistema receptor que la siguiente parte de la comunicación será el cuerpo real del mensaje de correo electrónico. Cuando el sistema conectado finaliza de enviar el mensaje de correo electrónico, coloca un punto sencillo (`.`) en una línea. A partir de ese momento, se considera que el mensaje se ha enviado.

El protocolo SMTP también permite gestionar el reenvío de mensajes entre sistemas si el sistema receptor sabe el destino al que tiene que enviar el mensaje. El protocolo puede verificar si determinados usuarios utilizan realmente un servidor de correo concreto (comando `VRFY`) o ampliar una lista de distribución de correo (comando `EXPN`). También se puede retrasar el envío de correo electrónico entre dos servidores SMTP si en los dos sistemas se permite realizar esta actividad.

A diferencia de los protocolos IMAP y POP, el protocolo SMTP no requiere autenticación en su forma más básica. Esto ha provocado mucho correo basura o spam, ya que un usuario no local puede utilizar el sistema de otro para enviar o transmitir el correo a listas completas de destinatarios con los recursos y ancho de banda del sistema. Las aplicaciones SMTP modernas han progresado enormemente al minimizar este comportamiento y restringir las transmisiones de modo que sólo los hosts conocidos envíen correo electrónico.

En el documento RFC-821 se describe el comportamiento básico del protocolo SMTP, aunque varias extensiones de SMTP, posibles gracias a RFC-1869, han agregado nuevas funciones al SMTP a lo largo de los años con nuevos comandos. Al iniciar una conversación con un servidor SMTP mediante un comando `EHLO`, en lugar de `HELO`, el servidor conectado puede identificarse a sí mismo como un servidor compatible con las extensiones SMTP. El servidor receptor contesta con una línea `250` que contiene las distintas extensiones SMPT compatibles. A continuación, el servidor conectado puede utilizar las extensiones compatibles como desee para obtener los objetivos de la comunicación.

Una de las extensiones que merece la pensa destacar está relacionada con la incorporación de autenticación SMTP mediante el comando `AUTH`, tal y como se describe en el documento RFC-2554. Otra extensión SMTP muy utilizada se explica en detalle en el documento RFC-2034, que describe el uso entre aplicaciones SMTP de códigos de error estándar separados por puntos. La lectura de los documentos RFC en los que se describen aspectos del protocolo SMTP proporciona los conocimientos básicos sobre la forma de transferir el correo electrónico en Internet. Además, puede conectarse a un servidor SMTP mediante telnet si especifica el puerto 25, como, por ejemplo `telnet localhost 25`. Ejecute varios comandos y envíe correos electrónicos manualmente para aprender cómo funcionan las comunicaciones SMTP.

Red Hat Linux utiliza Sendmail (`/usr/sbin/sendmail`)como programa SMTP por defecto, aunque hay disponibles otras aplicaciones con funciones similares pero de más fácil uso, como Postfix (`/usr/sbin/sendmail`). Consulte Sección 15.2.2 para mayor información.

15.2. Diferentes tipos de programas de correo electrónico

Hay tres tipos de programas de correo electrónico y todos ellos desempeñan un papel específico en el proceso de trasmitir y administrar mensajes de correo electrónico. Aunque la mayoría de los usuarios sólo conocen el programa de correo electrónico con el sistema para enviar y recibir mensajes, cada uno de los tipos de programas siguientes es también importante para garantizar que los mensajes llegan al destino correcto.

15.2.1. MUA (Mail User Agent, Agente de usuario de correo)

Un *MUA (Mail User Agent, Agente de usuario de correo)* es un programa que permite a un usuario, como mínimo, leer y escribir mensajes de correo electrónico. A un MUA se le denomina a menudo *cliente de correo*. Lógicamente, hay muchos programas MUA que ofrecen al usuario muchas más funciones, entre las que se incluyen la recuperación de mensajes mediante los protocolos POP e IMAP, la configuración de buzones de correo para almacenar los mensajes o ayuda para presentar los mensajes nuevos a un programa MTA (Mail Transfer Agent, Agente de transferencia de correo) que los enviará al destino final.

Los programas MUA pueden ser gráficos, como **Mozilla Mail**, o pueden tener una interfaz basada en texto sencilla, como **Mutt** o **Pine**.

15.2.2. MTA (Mail Transfer Agent, Agente de transferencia de correo)

Un programa *MTA (Mail Transfer Agent, Agente de transferencia de correo)* transfiere los mensajes de correo electrónico entre máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar al destino final. La mayoría de los usuarios desconocen la existencia de estos agentes, incluso si cada mensaje se envía a través de como mínimo un MTA.

Aunque el proceso de envío de mensajes entre las máquinas pueden parecer bastante directo, todo el proceso de decidir si un agente MTA concreto puede o debe aceptar un mensaje para entregarlo a un host remoto es bastante complicado. Además, debido a los problemas de correo basura, el uso de un MTA concreto normalmente está limitado por la propia configuración del MTA o el acceso a la red del sistema que lo ejecuta.

Muchos de los agentes MUA de mayores dimensiones y complejidad también sirven para enviar correo. Sin embargo, no se debe confundir esta acción con las funciones propias y verdaderas de estos agentes. Para que los usuarios que no ejecutan un agente MTA propio puedan transmitir los mensajes salientes a una máquina remota para su envío, deben utilizar una capacidad en el MUA capaz de transferir el mensaje a un MTA para el que tengan autorización de uso. Sin embargo, el agente MUA no entrega directamente el mensaje al servidor de correo del destinatario final; esta función está reservada al agente MTA.

Red Hat Linux utiliza Sendmail como agente MTA por defecto, aunque se pueden utilizar otros muchos en su lugar.

Nota

Para saber cómo cambiar MTA predeterminado con el Sendmail al Postfix, vea el capítulo *Configuración del Mail Transport Agent (MTA)* en el *Manual oficial de personalización de Red Hat Linux*.

15.2.3. MDA (Mail Delivery Agent, Agente de entrega de correo)

Los agentes MTA utilizan programas *MDA (Mail Delivery Agent, Agente de entrega de correo)* para entregar el correo electrónico al buzón de un usuario concreto. En muchos casos, el agente MDA es

realmente un *LDA (Local Delivery Agent, Agente de entrega local)*, como `bin/mail` o Procmail. Sin embargo, Sendmail también puede desempeñar la función de un agente MDA, como cuando acepta un mensaje de un usuario local y lo adjunta a su fichero de spool de correo electrónico. Cualquier programa que gestione realmente un mensaje para entregarlo al punto donde lo leerá un agente MUA se puede considerar un agente MDA. Tenga en cuenta que los agentes MDA no transportan mensajes entre sistemas ni actúan como interfaz para el usuario final.

Muchos usuarios no utilizan directamente agentes MDA, porque sólo se necesitan agentes MTA y MUA para enviar y recibir correo. Sin embargo, algunos agentes MDA se pueden utilizar para ordenar los mensajes antes de que los lea el usuario, lo cual es de gran ayuda si recibe una gran cantidad de correo.

15.3. Sendmail

Red Hat Linux usa Sendmail como agente MTA para la entrega de los mensajes, ya estén destinados a usuarios del mismo sistema o a usuarios ubicados en destinos remotos. No hay otro agente MTA (y su uso con Red Hat Linux es adecuado), pero la mayoría de los administradores deciden usar Sendmail como agente MTA por su eficacia, escalabilidad y cumplimiento con los estándares de Internet más importantes, como el protocolo SMTP.

La función principal de Sendmail, al igual que la de otros agentes MTA, es transferir de forma segura los correos electrónicos entre los hosts, normalmente mediante el uso del protocolo SMTP. Sin embargo, Sendmail es altamente configurable y permite controlar casi cada aspecto de cómo se gestiona el correo, incluido el protocolo que se va a utilizar.

15.3.1. Historia

Las raíces de Sendmail se remontan al nacimiento del correo electrónico, una década antes de que naciese ARPANET, el precursor de Internet. Por entonces, cada buzón de usuario era un fichero con derechos de sólo lectura y las aplicaciones de correo eran simplemente texto incorporado en ese fichero. Cada usuario tenía que abrir y meterse de lleno en el fichero de correo para buscar correos antiguos y leer el correo nuevo era toda una faena. La primera transferencia real de un fichero de mensaje de correo entre dos hosts no tuvo lugar hasta 1972, año en el que el correo electrónico empezó a transferirse por FTP a través de un protocolo de red NCP. Este método de comunicación más sencillo muy pronto se hizo popular, incluso hasta el punto de representar la mayor parte del tráfico de ARPANET en menos de un año.

Sin embargo, la falta de estándares entre los protocolos existentes convirtió al correo electrónico en más difícil de enviar desde algunos sistemas y así continuó hasta que ARPANET creó el estándar TCP/IP en 1982. Un nuevo protocolo, SMTP, que se materializaba en el transporte de mensajes. Estos avances, en combinación con la sustitución de los ficheros HOSTS por DNS, permitieron que se materializasen los agentes MTA con funciones completas. Sendmail, que creció a partir de un precedente sistema de entrega de correo electrónico denominado Delivermail, muy pronto se convirtió en estándar a medida que Internet comenzaba a expandirse y a utilizarse más ampliamente.

15.3.2. Objetivo y limitaciones

Es importante saber qué es Sendmail y qué le permite realizar y qué no. En estos días en los que las aplicaciones monolíticas pueden realizar varias funciones, se puede pensar inicialmente que Sendmail es la única aplicación que se necesita para ejecutar un servidor de correo electrónico dentro de la organización. Técnicamente es verdad que Sendmail puede enviar correo a los directorios de usuarios y aceptar nuevo correo mediante una línea de comandos, pero la mayoría de los usuarios necesitan mucho más que simplemente enviar correo electrónico. Normalmente desean interactuar con el correo mediante un agente MUA que utilice el protocolo POP o IMAP para descargar los mensajes en las

máquinas locales. O tal vez prefieren disponer de una interfaz Web que les proporcione acceso a sus buzones. Estas otras aplicaciones pueden ejecutarse en combinación con Sendmail y SMTP, pero realmente existen por otras razones y se pueden ejecutar de forma separada.

El objeto de esta sección es profundizar en cómo debería o podría configurarse Sendmail para realizar ciertas funciones. Puesto que este programa cuenta con prácticamente miles de opciones y conjuntos de reglas diferentes, hay innumerables documentos que tratan de explicar todo lo que se puede hacer y cómo solucionar los problemas. Es recomendable que consulte todas las fuentes de información disponibles en línea sobre Sendmail para darle forma y poder ajustar así este programa de modo que responda a las especificaciones exactas que precisa.

Sin embargo, es necesario que entienda qué ficheros se instalan por defecto con Sendmail en el sistema, así como aprender a realizar cambios básicos de configuración. Asimismo, es conveniente que sepa cómo detener correo no deseado (correo basura o spam) y cómo ampliar Sendmail con el protocolo *LDAP (Lightweight Directory Access Protocol, Protocolo ligero de acceso a directorios)*.

15.3.3. Instalación por defecto de Sendmail

Aunque se puede descargar el código fuente de Sendmail y crear una copia propia, muchos usuarios prefieren utilizar la versión de Sendmail que se instala por defecto con el sistema Red Hat Linux. Puede utilizar los CD-ROM de Red Hat Linux para volver a instalar el RPM de `sendmail` en un momento posterior. Tenga en cuenta que tiene que alterar el fichero de configuración predeterminado para el Sendmail que deba usar como servidor de correo electrónico para más de un host local. Vea Sección 15.3.4 para más detalles.

Después de la instalación, el fichero ejecutable `sendmail` se guarda en el directorio `/usr/sbin`.

El fichero de configuración, extenso y detallado, de Sendmail (`sendmail.cf`) se instala en `/etc`. No debe modificar el fichero `sendmail.cf` directamente salvo si sabe realmente lo que está haciendo, ya que es muy grande y complejo. En su lugar, cambie la configuración de Sendmail, modifique el fichero `/etc/mail/sendmail.mc` y utilice el procesador de macros `m4` que se incluye en el sistema para crear un nuevo fichero`/etc/sendmail.cf` (lógicamente, después de hacer una copia de seguridad del fichero original `/etc/sendmail.cf`). Si desea obtener más información sobre la configuración de Sendmail, consulte la Sección 15.3.4.

Se instalan varios ficheros de configuración de Sendmail en `/etc/mail`, entre los que se incluyen:

- `access` — Especifica los sistemas que puede utilizar Sendmail para enviar correo electrónico.
- `domaintable` — Le permite crear asignaciones de nombres de dominio.
- `local-host-names` — Ubicación en la que puede guardar todos los alias de la máquina.
- `mailertable` — Especifica las instrucciones para sobrescribir la ruta de determinados dominios.
- `virtusertable` — Le permite realizar una forma específica de dominio de alias con la que se pueden ubicar varios dominios virtuales en una máquina.

Algunos de los ficheros de configuración de `/etc/mail`, como, por ejemplo, `access`, `domaintable`, `mailertable` y `virtusertable`, deben almacenar realmente la información que contienen en los ficheros de base de datos para que Sendmail pueda utilizar cualquier cambio de configuración. Para incluir cualquier cambio realizado en estas configuraciones en los ficheros de bases de datos, debe ejecutar el comando `makemap hash /etc/mail/<nombre> < /etc/mail/<nombre>`, donde *<nombre>* es el nombre del fichero de configuración que debe convertirse.

Por ejemplo, si desea que todos los correos dirigidos a cualquier cuenta de `domain.com` se envíen a <bob@otherdomain.com>, tendrá que añadir una línea en el fichero `virtusertable`:

```
@domain.com       bob@otherdomain.com
```

Figura 15-1. Ejemplo de `virtusertable`

A continuación, añada la siguiente información al fichero `virtusertable.db` y ejecute `makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable` como root. Esto creará un nuevo fichero `virtusertable.db` que contiene la nueva configuración.

15.3.4. Cambios de configuración comunes de Sendmail

Se instalará el fichero `sendmail.cf` en `/etc` durante la instalación, tendrá que alterarlo para poder utilizar otras características y utilidades más avanzadas.

Cuando cambie el fichero de confifuración de Sendmail, es mejor que cree un fichero `/etc/sendmail.cf` completamente nuevo en vez de modifcar el ya existente.

Importante

Antes de modificar el fichero `sendmail.cf` haga una copia de seguidad de la versión predeterminada.

Para añadir la funcionalidad deseada a Sendmail, modifique el fichero `/etc/mail/sendmail.mc`. Despué use el procesador de macros `m4` para generar un fichero `sendmail.cf` nuevo ejecutando el comando `m4 /etc/mail/sendmail.mc > /etc/sendmail.cf`. Después de crear un nuevo fichero `/etc/sendmail.cf`, reinicie Sendmail para aplicar los cambios. La manera más sencilla de realizar esto es escribiendo el comando `/sbin/service sendmail restart` como raíz.

Por defecto, el procesador de macros `m4` se instala con Sendmail. El procesador de macros `m4` se incluye con el paquete `sendmail-cf`, que se instala en `/usr/share/sendmail-cf`.

Importante

El fichero predeterminado `sendmail.cf` no permite al sendmail aceptar las conexiones de red de cualquier host sino solamente de los ordenadores locales. Si desea configurar el sendmail como servidor para otros clientes, modifique `/etc/mail/sendmail.mc` y cambie `DAEMON_OPTIONS` para poder escuchar en los dispositivos de la red o comente esta opción. Despueés regenere el fichero `/etc/sendmail.cf` ejecutando:

Este tipo de configuración funciona solamente en los sitios SMTP. *No* funciona en los sitios UUCP a los sitios UNIX a copia de UNIX); tendrá que crear un nuevo `sendmail.cf` si quiere que se lleven a cabo las transferencias de correo UUCP.

Consulte el fichero `/usr/share/sendmail-cf/README` antes de modificar cualquier fichero del directorio `/usr/share/sendmail-cf`, ya que podría afectar a cómo están configurados los ficheros `/etc/sendmail.cf`.

15.3.4.1. Creación de máscaras

Una configuración común de Sendmail es disponer de una única máquina que actúe como gateway o pasarela de correo para todas las máquinas de la red. Por ejemplo, una empresa puede estar interesada en que la máquina denominada `mail.bigcorp.com` gestione todo el correo.

En esta situación, el servidor de correo electrónico necesita enmascarar los nombres de la máquina en la red de la empresa de manera que la dirección de vuelta sea user@bigcorp.com en vez de user@devel.bigcorp.com.

Para ello añda las siguientes líneas al directorio `/etc/mail/sendmail.mc`.

```
FEATURE(always_add_domain)dnl
FEATURE('masquerade_entire_domain')
FEATURE('masquerade_envelope')
FEATURE('allmasquerade')
MASQUERADE_AS('bigcorp.com.')
MASQUERADE_DOMAIN('bigcorp.com.')
MASQUERADE_AS(bigcorp.com)
```

Después de generar el nuevo `sendmail.cf` con el comando `m4`, esta configuración hará que todo el correo electrónico interno a la red parezca como si se hubiera mandado desde `bigcorp.com`.

15.3.5. Detener el correo basura con Sendmail

El *correo basura* se puede definir como el correo innecesario y no deseado que un usuario recibe, del que probablemente no conoce el remitente y al que nunca ha pedido una comunicación. Es un abuso muy negativo, costoso y de fácil expansión de los estándares de comunicación de Internet.

Sendmail ha hecho (relativamente) fácil bloquear las nuevas técnicas de correo basura que se utilizan para enviar este tipo de correo utilizando su sistema. Incluso bloquea muchos de los métodos usuales de correo basura por defecto. Necesitará activar el sistema adecuadamente, para lo cual deberá cambiar el fichero `/etc/mail/sendmail.mc` de un modo concreto para que el sistema sea susceptible.

Por ejemplo, el reenvío de mensajes SMTP, también conocido como *transmisión SMTP*, se ha desactivado por defecto desde la versión 8.9 de Sendmail. Antes de que se produjese este cambio, Sendmail pedía al host de correo (`x.org`) que aceptase los mensajes de una parte (`y.com`) y los mandase a otra parte (`z.net`). Ahora, no obstante, se debe indicar de forma específica a Sendmail que permita que un dominio transmita correo a través del dominio. Sólo debe modificar el fichero `/etc/mail/relay-domains` y reiniciar Sendmail para lo cual deberá escribir el comando `service sendmail restart` como raíz para que se apliquen los cambios.

Sin embargo, en muchas ocasiones, los usuarios reciben bombardeos de correo basura de otros servidores a través de Internet que usted puede controlar. En estos casos, puede utilizar las funciones de control de acceso de Sendmail que están disponibles en el fichero `/etc/mail/access`. Como raíz, agregue los dominios que desee bloquear o especifique los dominios con acceso, como, por ejemplo:

```
badspammer.com       550 Fuera y no mandes más correo basura
tux.badspammer.com   OK
10.0                 RELAY
```

Figura 15-2. Ejemplo de configuración para `access`

Puesto que `/etc/mail/access` es una base de datos, deberá usar el comando `makemap` para activar los cambios y recrear la asignación de la base de datos. Esto se realiza fácilmente ejecutando el comando `makemap hash /etc/mail/access < /etc/mail/access` como raíz.

Según este ejemplo, cualquier correo enviado por `badspammer.com` se bloqueará con un código de error 550 RFC-821 y se devolverá el mensaje al destinatario del correo basura, excepto si se ha enviado desde el subdominio `tux.badspammer.com`, que se aceptará. La última línea indica que cualquier correo enviado por la red 10.0.*.* se puede transmitir a través del servidor de correo.

Como puede imaginarse, este ejemplo sólo analiza una mínima parte de lo que Sendmail puede realizar en cuanto a permitir o bloquear el acceso. Consulte `/usr/share/doc/sendmail/README.cf` para obtener más información y ejemplos.

15.3.6. Uso de Sendmail con LDAP

El uso del protocolo *LDAP (Lightweight Directory Access Protocol, Protocolo ligero de acceso a directorios)* proporciona un medio rápido y eficaz de buscar información específica sobre un usuario concreto que forma parte de un grupo mayor. Puede usar, por ejemplo, un servidor LDAP para buscar una dirección de correo determinada en un directorio común de la empresa si especifica el apellido del usuario. En este tipo de implantación, LDAP es bastante independiente de Sendmail, en tanto LDAP almacena la información del usuario jerárquicamente y Sendmail sólo recibe el resultado de las consultas de LDAP en mensajes de correo previamente enrutados.

Sin embargo, Sendmail admite mucha más integración con LDAP y utiliza este protocolo para sustituir ficheros mantenidos independientemente, como `aliases` y `virtusertables`, que se ubican en servidores de correo diferentes. A modo de resumen, puede usar LDAP para extraer el nivel de enrutamiento de correo desde Sendmail y sus ficheros de configuración independientes en un cluster de LDAP que pueden utilizar distintas aplicaciones.

La versión actual de Sendmail es compatible con LDAP. Para ampliar el servidor de Sendmail y usar LDAP, primero debe obtener un servidor LDAP, como **OpenLDAP**, ejecutarlo y configurarlo correctamente. A continuación, modifique `/etc/mail/sendmail.mc` para incluir:

```
LDAPROUTE_DOMAIN('sudominio.com')dnl
FEATURE('ldap_routing')dnl
```

Figura 15-3. Ejemplo de configuración de LDAP en `sendmail.mc`

Nota

Esta es sólo una configuración muy básica de Sendmail con LDAP. La configuración puede ser muy diferente de la indicada según la implementación específica de LDAP, especialmente si desea configurar varias máquinas de Sendmail para que utilicen un servidor LDAP común.

Consulte `/usr/share/doc/sendmail/README.cf` para obtener instrucciones y ejemplos de configuración de enrutamiento de LDAP.

A continuación, vuelva a crear el fichero `/etc/sendmail.cf`. Para ello, ejecute `m4` y reinicie Sendmail. Consulte la Sección 15.3.4 para obtener más instrucciones sobre cómo realizar esto.

Para obtener más información sobre LDAP, consulte el Capítulo 18.

15.4. Fetchmail

Fetchmail es un programa que puede recuperar correo electrónico de servidores remotos para conexiones TCP/IP bajo demanda. Muchos usuarios aprecian la capacidad de separar el proceso de descarga de mensajes ubicados en un servidor remoto del proceso de lectura y organización de correo en un MUA. Se ha diseñado teniendo presente las necesidades de los usuarios de acceso telefónico a redes. Fetchmail se conecta y descarga rápidamente todos los mensajes al fichero spool de correo mediante el uso de diversos protocolos, entre los que se incluyen POP3 e IMAP. Incluso permite reenviar los mensajes de correo a un servidor SMTP si es necesario.

Antes de intentar usar Fetchmail, compruebe que está instalado en el sistema. Si no lo está, utilice el RPM de `fetchmail` que está disponible en los CD-ROM de Red Hat Linux.

La configuración de Fetchmail se realiza en el fichero `.fetchmailrc`, ubicado en el directorio principal del usuario. Hay un programa asociado con Fetchmail, denominado `fetchmailconf`, que es muy útil para configurar de forma básica el fichero `.fetchmailrc`.

Mediante el uso de preferencias en el fichero `.fetchmailrc`, Fetchmail comprobará si hay correo en un servidor remoto e intentará entregarlo al puerto 25 de la máquina local utilizando el agente MTA local para dirigir el correo al fichero de spool del usuario correcto. Si también está disponible Procmail, podrá utilizarlo para filtrar el correo y colocarlo en un buzón para que lo pueda leer un MUA.

15.4.1. Opciones de configuración de Fetchmail

Aunque se pueden insertar todas las opciones en la línea de comandos pertinente para comprobar si hay correo en un servidor remoto al ejecutar Fetchmail, el uso de `.fetchmailrc` proporciona un método más sencillo. Todas las opciones de configuración se guardan en el fichero `.fetchmailrc`, pero se pueden sobrescribir cuando se ejecuta Fetchmail si se especifica esta opción en la línea de comandos.

Un fichero de usuario `.fetchmailrc` se divide en tres tipos concretos de opciones de configuración:

- *Opciones globales* — Indican a Fetchmail las instrucciones que controlan el funcionamiento del programa o proporcionan los valores para cada conexión en la que se comprueba si hay correo electrónico.
- *Opciones de servidor* — Especifican información necesaria sobre el servidor, como nombre de host, así como las preferencias que desearía ver aplicadas con un servidor de correo concreto, como el puerto en el que se deben comprobar el número de segundos de espera antes de un timeout. Estas opciones afectan a cada opción de usuario utilizada con ese servidor.
- *Opciones de usuario* — Contienen información, como nombre de usuario y contraseña, que es necesaria para autenticar y comprobar si hay correo utilizando un servidor de correo concreto.

Las opciones globales se encuentran en la parte superior del fichero `.fetchmailrc`, seguidas de una o varias opciones de servidor con las que se designa cada uno de los servidores de correo diferentes que debería comprobar Fetchmail. Por último, se encuentran las opciones de usuario específicas de cada cuenta de usuario que desea comprobar en el servidor de correo. Al igual que las opciones de servidor, se pueden especificar varias opciones de usuario para utilizarlas con un servidor determinado (por ejemplo, si desea comprobar varias cuentas de correo electrónico en el mismo servidor).

Las opciones de servidor se llaman para ejecución en el fichero `.fetchmailrc` si se especifica un verbo de opción especial, `poll` o `skip`, que precede a cualquier otra información del servidor. La acción `poll` indica a Fetchmail que se debe utilizar esta opción de servidor cuando se ejecute y compruebe si hay correo utilizando las distintas opciones de usuario. Sin embargo, no se comprueba ninguna opción de servidor que esté situada después de la acción `skip`, salvo si se especifica este nombre de host al llamar a Fetchmail. La opción `skip` le permite definir configuraciones de prueba en `.fetchmailrc` y sólo comprueba el uso de ese servidor cuando se especifica en concreto sin que resulten afectadas otras configuraciones actuales.

Un fichero `.fetchmailrc` de ejemplo tiene el aspecto siguiente:

```
set postmaster "user1"
set bouncemail

poll pop.domain.com proto pop3
     user 'user1' there with password 'secret' is user1 here
```

```
poll mail.domain2.com
     user 'user5' there with password 'secret2' is user1 here
     user 'user7' there with password 'secret3' is user1 here
```

Figura 15-4. Ejemplo de fichero básico `.fetchmailrc`

En este ejemplo, las opciones globales son las que establecen que se le envíe correo al usuario como última instancia (opción `postmaster`) y que todos los errores de correo se manden al postmaster en lugar de a la persona que ha enviado el correo `bouncemail`). La acción `set` indica a Fetchmail que esta línea contiene una opción global. A continuación, se especifican dos servidores de correo: uno para que compruebe si hay correo con el protocolo POP3 y otro para que pruebe a usar varios protocolos para encontrar uno que funcione. Se comprueba el correo de dos usuarios con la segunda opción de servidor, pero todo el correo que se encuentre se envía al spool de correo del user1. Esto permite comprobar varios buzones de diversos servidores como si se tratara de un único buzón MUA. La información específica de cada usuario comienza con la acción `user`.

Nota

No es necesario que especifique la contraseña en el fichero `.fetchmailrc`. Puede omitir la sección `with password '<password>'`. Fetchmail le pedirá la contraseña cuando se inicie con el comando `fetchmail`.

Aunque puede configurar manualmente el fichero `.fetchmailrc`, es más sencillo que el programa `fetchmailconf` lo realice. Sin embargo, al realizar pruebas de las nuevas configuraciones, suele ser más fácil modificar el fichero `.fetchmailrc` directamente.

Como se puede esperar de un programa que ofrece tales servicios de red como correo y que utiliza tantos protocolos, Fetchmail contiene diferentes opciones globales, de servidor y locales. Muchas de estas opciones sólo se utilizan puntualmente o son válidas para situaciones muy concretas. La página man de `fetchmail` explica cada una de estas opciones en profundidad, pero las más comunes se describen aquí.

15.4.1.1. Opciones globales

Cada opción global debe colocarse en una línea única después de una acción `set`.

- `daemon <segundos>` — Indica a Fetchmail de usar automáticamente el modo de demonio, con el que estará en segundo plano y comprobar si hay correo en los intervalos especificados.
- `postmaster` — Indica a Fetchmail un usuario local para enviar el correo en caso de problemas de entrega.
- `syslog` — Indica a Fetchmail de iniciar el registro de mensajes de error y de estado en el fichero .log del sistema. Por defecto, es el fichero `/var/log/maillog`.

15.4.1.2. Opciones del servidor

Escriba las opciones del servidor en la propia línea en `.fetchmailrc` después de una acción `poll` o `skip`.

- `auth <auth-type>` — Especifica el tipo de autenticación que se utilizará. Por defecto, se utiliza la autenticación por `password` pero algunos protocolos admiten también otros tipos, entre los que se incluyen `kerberos_v5`, `kerberos_v4`y `ssh`. Si se usa el tipo de autenticación `any`, Fetchmail primero usará métodos que no necesiten contraseña y luego otros que creen máscara para la contraseña. Finalmente, intentará enviar la contraseña como medio de autenticar el servidor.

- `interval <número>` — Indica a Fetchmail de sólo comprobar el servidor cada cierto `<número>` de veces en todos los servidores configurados. Esta opción se puede usar con servidores de correo a través de los que reciba raramente mensajes.
- `port <número de puerto>` — Sobrescribe el número de puerto por defecto de un protocolo especificado.
- `proto <protocolo>` — Indica a Fetchmail de usar un protocolo específico, como `pop3` o `imap`, para comprobar los mensajes del servidor.
- `timeout<segundos>` — Configura Fetchmail para abandonar después de un determinado intervalo de inactividad del servidor. Si no se define este valor, se asume un valor de `300` segundos.

15.4.1.3. Opciones de usuario

Las opciones de usuario se pueden insertar en las propias líneas debajo de una opción de servidor en la misma línea que la opción de servidor. En cualquier caso, las opciones de usuarios van después de la opción `user` (definida más abajo).

- `fetchall` — Ordena a Fetchmail descargar todos los mensajes en cola, incluidos los mensajes que ya se han visto. Por defecto, Fetchmail sólo lo hace con los nuevos.
- `fetchlimit <número>` — Sólo permite descargar un determinado número de mensajes antes de detenerse.
- `flush` — Indica a Fetchmail de eliminar todos los mensajes en cola que ya se han visto antes de descargar mensajes nuevos.
- `limit <número máx. bytes>`— Permite especificar que sólo se recuperen los mensajes de una tamaño inferior al indicado. Esta opción es útil para reducir las conexiones de red, cuando puede tardar mucho en descargarse un mensaje de gran tamaño.
- `password '<contraseña>'` — Especifica la contraseña que utilizará este usuario.
- `preconnect "<comando>"` — Indica a Fetchmail de ejecutar el comando especificado antes de recuperar los mensajes de este usuario.
- `postconnect "<comando>"` — Indica a Fetchmail de ejecutar el comando especificado después de recuperar los mensajes de este usuario.
- `ssl` — Permite a Fetchmail recopilar los mensajes mediante una conexión SSL cifrada si el servidor la admite.
- `user "<nombre de usuario>"` — Establece el nombre de usuario que Fetchmail usa para recuperar los mensajes. Esta opción debe aparecer antes de cualquier otra opción de usuario.

15.4.2. Opciones de comando de Fetchmail

La mayoría de las opciones de Fetchmail se pueden utilizar en la línea de comando al ejecutar el comando `fetchmail` o reflejar las opciones de configuración de `.fetchmailrc`. Esto se realiza para que se use Fetchmail con o sin un fichero de configuración. La mayoría de los usuarios usan estas opciones en la línea de comandos porque les resulta más sencillo dejarlas en el fichero `.fetchmailrc` para que se utilicen cada vez que se ejecuta Fetchmail.

Sin embargo, en ocasiones puede estar interesado en ejecutar el comando `fetchmail` con otras opciones para un fin concreto. Puesto que cualquier opción especificada en la línea de comando sobrescribe las opciones del fichero de configuración, puede omitir opciones de comando temporales que sobrescriban un parámetro de `.fetchmailrc` que causa un error.

15.4.2.1. Opciones informativas o de depuración

Determinadas opciones que se utilizan después del comando `fetchmail` pueden proporcionar información importante.

- `--configdump` — Muestra cada opción posible en función de la información de `.fetchmailrc` y los valores por defecto de Fetchmail. No se recupera correo de ningún usuario al usar esta opción.
- `-s` — Ejecuta Fetchmail en modo silencioso, con lo cual se evita que aparezcan mensajes y errores después del comando `fetchmail`.
- `-v` — Ejecuta Fetchmail en modo detallado y muestra todas las comunicaciones entre Fetchmail y los servidores de correo remotos.
- `-V` — Hace que Fetchmail muestre información de versión detallada, una lista de las opciones globales y los parámetros que se utilizarán con cada usuario, incluido el protocolo de correo y el método de autenticación. No se recupera correo de ningún usuario al usar esta opción.

15.4.2.2. Opciones especiales

Estas opciones son en ocasiones útiles para sobrescribir los valores por defecto que a menudo contiene el fichero `.fetchmailrc`.

- `-a` — Indica a Fetchmail de descargar todos los mensajes del servidor de correo remoto, ya se hayan o no visto antes. Por defecto, Fetchmail sólo descarga los mensajes nuevos.
- `-k` — Hace que Fetchmail deje una copia de los mensajes en el servidor de correo remoto después de descargarlos. Esta opción sobrescribe el comportamiento por defecto de eliminar los mensajes después de descargarlos.
- `-l` *<número máximo de bytes>*— Indica a Fetchmail que no descargue mensajes con un tamaño superior al indicado y dejarlos en el servidor de correo remoto.
- `--quit` — Sale del proceso de demonio de Fetchmail.

Hay más comandos y opciones de `.fetchmailrc` en la página man de `fetchmail`.

15.5. Procmail

Procmail le permite filtrar el correo a medida que lo recibe de un servidor de correo remoto o colocarlo en el fichero spool de un servidor de correo local o remoto. Es una herramienta eficaz, que hace un uso adecuado de los recursos del sistema y de amplio uso. Procmail, comúnmente denominado *LDA (Local Delivery Agent. Agente de entrega local)*, desempeña una pequeña función en la entrega de correo para su lectura por un agente MUA.

Para utilizarlo, primero deberá instalarlo. Escriba el comando `rpm -q procmail` para ver si tiene instalado el paquete `procmail`. Si, por alguna razón, Procmail no está en el sistema, instálelo utilizando los CD-ROM de instalación de Red Hat Linux.

Procmail se puede llamar de distintos modos. Puesto que el correo se ubica en el fichero spool de correo electrónico, Procmail se puede configurar para arrancar, filtrar el correo en las ubicaciones configuradas para utilizar con el agente MUA y salir. Opcionalmente, puede configurar el agente MUA para iniciar Procmail en cualquier momento que se reciba un mensaje para que los mensajes se trasladen a los buzones correctos. En muchos casos, la presencia de un fichero `.procmailrc` en el directorio principal del usuario llamará la actividad de Procmail, si se utiliza Sendmail.

Las acciones que Procmail realiza con el correo dependen de las instrucciones de las *recetas* o reglas mediante las que se comparan los mensajes con el programa. Si un mensaje coincide con la receta o regla, el correo se ubicará en un determinado fichero, se eliminará o se procesará.

Cuando Procmail arranca, lee el mensaje de correo y separa el cuerpo de la información de cabecera. A continuación, busca el fichero `/etc/procmailrc` y los ficheros `rc` en el directorio por defecto `/etc/procmailrcs` de todo el sistema, así como las variables y reglas de entorno. Luego busca si hay un fichero `.procmailrc` en el directorio principal del usuario para encontrar las reglas específicas de dicho usuario. Muchos usuarios también crean ficheros `rc` adicionales propios para Procmail que utilizan el fichero `.procmailrc`, pero que se pueden activar o desactivar rápidamente si se produce un problema al filtrar el correo.

Por defecto, no hay ficheros `rc` aplicables a todo el sistema en el directorio `/etc` y tampoco hay ficheros `.procmailrc`. Para empezar a usar Procmail, deberá crear un fichero `.procmailrc` con variables y reglas de entorno concretas que expliquen lo que deberá realizarse con determinados mensajes.

En la mayoría de las configuraciones, la decisión sobre si Procmail se arranca e intenta filtrar el correo se basa en el existencia de un fichero de usuario `.procmailrc`. Para desactivar Procmail, pero guardar el trabajo en el fichero `.procmailrc`, copie la información a un fichero de nombre similar que utilice el comando `mv ~/.procmailrc ~/.procmailrcSAVE`. Cuando esté preparado para realizar nuevas pruebas con Procmail, cambie nuevamente el nombre del fichero a `.procmailrc`. Procmail empezará a funcionar de nuevo inmediatamente.

15.5.1. Configuración de Procmail

Los ficheros de configuración de Procmail, y más en concreto el fichero de usuario `.procmailrc`, contienen variables de entorno importantes. Estas variables indican a Procmail qué mensajes deben ordenarse, qué hacer con los mensajes que no coinciden con ninguna receta, etc.

Estas variables de entorno normalmente aparecen al principio del fichero `.procmailrc` con el siguiente formato en cada línea:

<env-variable>="*<value>*"

Figura 15-5. Estructura de la línea de la variable de entorno

En este ejemplo, *<env-variable>* es el nombre de la variable y *<valor>* define la variable.

Muchas variables de entorno no se utilizan por la mayor parte de los usuarios de Procmail, y muchas de las variables de entorno más importantes ya están definidas con un valor por defecto. La mayoría del tiempo tratará con las siguientes variables:

- `DEFAULT` - Establece el buzón por defecto en el que se ubicarán los mensajes que no coincidan con las recetas.

  El valor por defecto `DEFAULT` es el mismo que `$ORGMAIL`.

- `INCLUDERC` - Especifica ficheros `rc` adicionales que contienen más recetas para los que deben comprobarse los mensajes. Esto permite desglosar las listas de recetas de Procmail en ficheros individuales según diversas funciones (como bloquear correo basura y gestionar listas de correo) que se pueden activar o desactivar con caracteres de comentario en el fichero de usuario `.procmailrc`.

  Por ejemplo, el aspecto de dos líneas del fichero de usuario `.procmailrc` puede ser el siguiente:

  ```
  MAILDIR=$HOME/Msgs
  INCLUDERC=$MAILDIR/lists.rc
  INCLUDERC=$MAILDIR/spam.rc
  ```

  Si el usuario desea desactivar el filtro de Procmail para las listas de correo, pero quiere controlar el correo basura, solamente deberá comentar la primera línea `INCLUDERC` con un carácter #.

- `LOCKSLEEP` - Establece cada cuanto tiempo, en segundos, Procmail intentará usar un lockfile concreto. El valor por defecto es ocho segundos.
- `LOCKTIMEOUT` - Establece la cantidad de tiempo, en segundos, que debe transcurrir después de modificar un lockfile para que Procmail asuma que este lockfile es antiguo para que se pueda eliminar. El valor por defecto es 1024 segundos.
- `LOGFILE` - Ubicación y fichero que contienen los mensajes de error o de información de Procmail.
- `MAILDIR` - Establece el directorio de trabajo actual de Procmail. Si se define este directorio, todas las rutas de Procmail estarán relacionadas con este directorio.
- `ORGMAIL` - Especifica el buzón original u otro lugar para colocar los mensajes si no se pueden ubicar en la ubicación de receta o por defecto.

  Por defecto, se utiliza el valor de `/var/spool/mail/$LOGNAME`.
- `SUSPEND` - Establece la cantidad de tiempo, en segundos, que Procmail se detendrá si está disponible un recurso necesario, como espacio de intercambio.
- `SWITCHRC` - Permite a un usuario especificar un fichero externo que contiene recetas de Procmail adicionales, como la opción `INCLUDERC` , excepto si la receta en examen se ha detenido en el fichero de configuración de referencia y sólo se usan las recetas del fichero `SWITCHRC` especificado.
- `VERBOSE` - Hace que Procmail registre mucha más información. Esta opción es útil para procesos de depuración.

Otras variables de entorno importantes se extraen del shell, como `LOGNAME` que es el nombre de conexión, `HOME` que es la ubicación del directorio principal y `SHELL` que es el shell por defecto.

Hay una explicación completa de todas las variables de entorno y sus valores por defecto en la página man de `procmailrc`.

15.5.2. Recetas de Procmail

Los usuarios nuevos consideran que la creación de recetas es la parte más difícil de Procmail. En cierto modo, esto es lógico, ya que las recetas comparan los mensajes con las *expresiones regulares*, que es un formato concreto que se utiliza para especificar cualificaciones para un cadena coincidente. Sin embargo, las expresiones regulares no son difíciles de crear, e incluso es menos difícil comprenderlas que leerlas. Además, ser coherentes al desarrollar recetas de Procmail, independientemente de las expresiones regulares, facilita adivinar su contenido.

No entra en el objeto de este capítulo ofrecer una explicación extensa sobre las expresiones regulares. La estructura de las recetas de Procmail es más importante, y hay ejemplos útiles de ellas en varios sitios de Internet, por ejemplo en http://www.iki.fi/era/procmail/links.html. El uso y la adaptación adecuada de las expresiones regulares contenidas en estos ejemplos dependerá de si se entiende la estructura correspondiente. Hay disponible información básica específica de las reglas de expresiones regulares en la página man de `grep`.

Una receta de Procmail tiene la siguiente estructura:

```
:0<flags>: <lockfile-name>

* <special-condition-character> <condition-1>
* <special-condition-character> <condition-2>
* <special-condition-character> <condition-N>

<special-action-character><action-to-perform>
```

Figura 15-6. Estructura de una receta de Procmail

Los dos primeros caracteres de una receta de Procmail son dos puntos y un cero. Opcionalmente, se pueden insertar varios indicadores después del cero para controlar lo que hace Procmail cuando procesa la receta. Dos puntos después de la sección *<flags>* especifica que se creará un lockfile para este mensaje. Si se va a crear un lockfile, debe especificar su nombre en el espacio *<lockfile-name>*.

Una receta puede contener varias condiciones con las que se comparará el mensaje. Si no tiene condiciones, cada mensaje se comparará en función de la receta. Las expresiones regulares se insertan en algunas condiciones para facilitar su comparación con un mensaje. Si se usan varias condiciones, todas ellas deben coincidir para que se realice una acción. Las condiciones se comprueban en función de los indicadores establecidos en la primera línea de la receta. El uso de caracteres especiales opcionales que se insertan después del carácter * permiten controlar todavía más la condición.

La acción *<action-to-perform>* especifica lo que le ocurrirá a un mensaje si cumple una de las condiciones. Sólo puede haber una acción por receta. En muchos casos, se usa aquí el nombre de un buzón para dirigir los mensajes coincidentes a ese fichero con el fin de ordenar de una manera eficaz el correo. También se pueden usar caracteres de acción especiales antes de especificar la acción.

15.5.2.1. Recetas de entrega y de no entrega

La acción usada si la receta coincide con un mensaje concreto determina si la receta se considera de entrega o de no entrega. Una *receta de entrega* contiene una acción que registra el mensaje en un fichero, envía el mensaje a otro programa o reenvía el mensaje a otra dirección de correo. Una *receta de no entrega* cubre cualquier otra acción, como el uso de un bloque de anidamiento. Un *bloque de anidamiento* es una acción entre corchetes `{ }` que designa las acciones adicionales que deben realizarse en los mensajes que cumplen las condiciones de la receta. Los bloques de anidamiento pueden ser anidados, lo cual proporciona un mayor control a la hora de identificar y realizar acciones en los mensajes.

La entrega de recetas coincidentes con mensajes provoca que Procmail realice la acción especificada y detenga la comparación del mensaje con otras recetas. Los mensajes que cumplen las condiciones de las recetas de no entrega seguirán comparándose con otras recetas en los ficheros `rc`. En otras palabras, las recetas de no entrega, hacen que el mensaje siga pasando por las recetas después de adoptarse la acción especificada.

15.5.2.2. Indicadores

Los indicadores son muy importantes para determinar cómo se compararán las condiciones de una receta con un mensaje. Los siguientes indicadores son de uso común:

- `A` - Especifica que esta receta sólo se usará si la última receta anterior sin una receta `A` o `a` también coincide con este mensaje.

  Para garantizar que se ha completado correctamente la acción de la última receta coincidente anterior, antes de que se permita comparar la receta actual, utilice el indicador `a`.
- `B` - Analiza el cuerpo del mensaje y busca condiciones coincidentes.
- `b` - Utiliza el cuerpo de una acción resultante, como escribir el mensaje a un fichero o reenviarlo. Este es el comportamiento por defecto.
- `c` - Genera una copia CC del correo electrónico. Es útil para entrega a recetas, puesto que la acción necesaria se puede realizar en el mensaje y se puede seguir procesando una copia del mensaje en los ficheros `rc`.
- `D` - Hace una comparación `egrep` que distingue entre mayúsculas y minúsculas. Por defecto, el proceso de comparación no distingue entre mayúsculas y minúsculas.

- `E` - Similar al indicador `A`, con la diferencia de que las condiciones de la receta sólo se comparan con el mensaje si la receta inmediatamente anterior sin un indicador `E` no coincide. Se puede comparar con la acción *else*.

  Use el indicador `e` si sólo desea que se compruebe esta receta en el caso de que la receta anterior coincidiese pero fallase la acción.
- `f` - Usa la canalización como filtro.
- `H` - Analiza la cabecera del mensaje y busca condiciones coincidentes. Este es el comportamiento por defecto.
- `h` - Usa la cabecera en la acción resultante. Este es el comportamiento por defecto.
- `w` - Indica a Procmail que debe esperar a que finalice el proceso del filtro o programa especificado, y que cree un informe independientemente de si termina correctamente antes de considerar si el mensaje debe filtrarse.

  Si desea omitir los mensajes de "error de programa", cuando decida si un filtro o no termina correctamente, utilice la opción `W`.

Hay indicadores adicionales en la página man de `procmailrc`.

15.5.2.3. Especificación de un Lockfile local

Los ficheros lockfiles son muy útiles en Procmail para garantizar que no más de un proceso intenta alterar un mensaje concreto al mismo tiempo. Puede especificar un lockfile local si inserta un carácter `:` después de cualquier indicador en la primera línea de una receta. Con esto se creará un lockfile local basado en el nombre de fichero de destino más cualquier otro valor definido en la variable de entorno global `LOCKEXT`.

Como alternativa, puede especificar el nombre del lockfile local que se usará con esta receta después del carácter `:`.

15.5.2.4. Condiciones y acciones especiales

El uso de determinados caracteres antes de las condiciones y acciones de recetas de Procmail cambian el modo en que se interpretan.

Los siguientes caracteres se pueden usar después del carácter `*` al principio de una línea de condición de receta:

- `!` - Invierte la condición y ocasiona que sólo se produzca una coincidencia si la condición no coincide con el mensaje.
- `<` - Comprueba si el mensaje tiene un número inferior de bytes.
- `>` - Comprueba si el mensaje tiene un número superior de bytes.

Los siguientes caracteres se utilizan para realizar acciones especiales:

- `!` - Indica a Procmail que reenvíe el mensaje a las direcciones de correo especificadas.
- `$` - Hace referencia a una variable establecida anteriormente en el fichero `rc`. Se usa normalmente para establecer un buzón común que utilizarán varias recetas.
- `|` - Carácter de canalización que indica a Procmail que debe arrancar un programa específico para gestionar este mensaje.
- `{` and `}` - Crea un bloque de anidamiento que se usa en combinación con recetas adicionales para aplicarlo a los mensajes coincidentes.

Si no se utiliza un carácter especial al principio de la línea de acción, Procmail asume que la línea de acción está especificando un buzón donde registrar el mensaje.

15.5.2.5. Ejemplos de recetas

Procmail es un programa extremadamente flexible que permite comparar los mensajes con condiciones muy específicas y, a continuación, realizar en ellos acciones muy detalladas. Sin embargo, como resultado de esta flexibilidad, la composición de una receta de Procmail desde cero para alcanzar un objetivo concreto, puede resultar una labor muy complicada para los usuarios nuevos.

La mejor manera de obtener los conocimientos necesarios para crear condiciones de recetas de Procmail es comprender las expresiones regulares y analizar los distintos ejemplos de otros desarrolladores. Los siguientes ejemplos, muy básicos, servirán para mostrar la estructura de las recetas de Procmail y pueden proporcionar la base para crear otras recetas más complejas.

Las recetas más básicas ni tan siquiera contienen condiciones, como se demuestra en el Figura 15-7.

```
:0:
new-mail.spool
```

Figura 15-7. Ejemplo sin condiciones

La primera línea inicia la receta mediante la especificación de que se cree un lockfile local pero sin indicar un nombre, de modo que Procmail utilice el nombre del fichero de destino y `LOCKEXT` cree su nombre. No se especifica ninguna condición y, por tanto, cada mensaje se comparará con esta receta y se insertará en el fichero de spool exclusivo denominado `new-mail.spool`, que se encuentra dentro del directorio especificado por la variable de entorno `MAILDIR`. Un agente MUA verá a continuación los mensajes de este fichero.

Esta receta básica se insertará al final de todos los ficheros `rc` para dirigir los mensajes a una ubicación por defecto. Un ejemplo más complejo, que extrae los mensajes de una dirección de correo concreta y los saca, se puede ver en la Figura 15-8.

```
:0
* ^From: spammer@domain.com
/dev/null
```

Figura 15-8. Ejemplo de correo electrónico enviado a `/dev/null`

Con este ejemplo, cualquier mensaje enviado a `spammer@domain.com` se moverá inmediatamente a `/dev/null` y se eliminará.

Atención:

Tenga en cuenta que una regla funciona adecuadamente antes de mover los mensajes que coinciden con `/dev/null`, que supone una eliminación permanente. Si las condiciones de receta "atrapan" inadvertidamente mensajes no destinados correctamente, no sabrá si esos mensajes le faltan salvo si se lo indica el emisor del mensaje.

Una solución mejor es dirigir la acción de la receta a un buzón especial que compruebe de vez en cuando para buscar *positivos falsos* o mensajes que han coincidido inadvertidamente con las condiciones. Una vez comprobado que no se han comparado por error los mensajes, puede eliminar el buzón y dirigir la acción para enviar los mensajes a `/dev/null`.

Procmail se usa principalmente como filtro de correo que lo coloca automáticamente en el lugar correcto para que no tenga que ordenarlo manualmente. La receta de la Figura 15-9 extrae el correo enviado desde una lista de distribución concreta y lo coloca en la carpeta correcta.

```
:0: *
^(From|CC|To).*tux-lug tuxlug
```

Figura 15-9. Ejemplo de filtro de lista

Cualquier mensaje enviado desde la lista de distribución `tux-lug@domain.com` se colocará automáticamente en el buzón `tuxlug` para el agente MUA. Tenga en cuenta que la condición de este ejemplo comparará el mensaje si tiene la dirección de correo de la lista de distribución en las líneas `From`, `CC`, o `To`.

Procmail también se puede usar para bloquear el correo basura, pero esta no es una buena solución a largo plazo para deshacerse de este tipo de correo. Considere usar la solución para filtrar correo basura de forma temporal de Figura 15-10, en la que se definen varias recetas que utilizan un buzón común para almacenar el correo basura.

```
SPAM=junk

:0: * To??^$

:0: * ^(To|CC):.*,.*,.*,.*,.*,.*,.*,.*,.*,.*,

:0: * ^Message-Id:.*<[^@]*>
```

Figura 15-10. Ejemplo de un filtro de correo basura básico

En este ejemplo, el buzón `junk` está asociado a la variable `SPAM`, así que puede cambiar el buzón que contiene el correo basura a otro lugar. A continuación, tres recetas buscan mensajes para enviar el buzón `junk`.

La primera receta busca mensajes que no tienen destinatarios en la línea `To`. La segunda receta coteja cualquier mensaje que tenga 12 o más destinatarios. La primera receta busca mensajes con un ID de mensaje no válido.

Estos sencillos mensajes se han proporcionado para ayudarle a comenzar a crear recetas. Consulte los muchos recursos en línea sobre Procmail que hay disponibles en la Sección 15.7 para ver más recetas detalladas y eficaces.

15.6. Seguridad

Al igual que otros servicios existentes en una red no cifrada, la información de correo electrónico importante, como nombres de usuario, contraseñas y mensajes, se puede interceptar y ver sin que tenga conocimiento el servidor o el cliente de correo. Al usar los protocolos estándar POP e IMAP, toda la información de autenticación se envía "limpiamente", es decir, cualquier persona en la red entre el cliente y el servidor remoto puede ver esta información fácilmente.

15.6.1. Clientes de correo electrónico seguros

Afortunadamente, la mayoría de los agentes MUA de Linux están diseñados para comprobar el correo mediante SSL compatible con servidores de correo para cifrar los mensajes, de modo que se devuelvan

y envíen en la red. Para usar SSL al recuperar el correo, se debe activar esta opción en el cliente y en el servidor de correo.

SSL se activa muy fácilmente en el cliente, normalmente basta con pulsar un botón en el área de configuración del agente MUA. Los protocolos IMAP y POP seguros tienen números de puerto conocidos (993 y 995, respectivamente) que MUA utiliza para autenticar y descargar los mensajes.

Los agentes MUA más conocidos que se incluyen en Red Hat Linux, como **Mozilla Mail**, **Mutt** y **Pine**, ofrecen sesiones de correo electrónico cifradas con SSL.

15.6.2. Servidores de correo electrónico seguros

Ofrecer cifrado SSL a los usuarios de IMAP y POP del servidor de correo es muy sencillo. Red Hat Linux también incluye el paquete `stunnel`, que es un ajustador de cifrado SSL que ajusta el tráfico no seguro de red estándar de determinados servicios y que impide que los interceptores se "infiltren" en la comunicación entre el cliente y el servidor. Aunque el comando `stunnel` puede utilizarse con más de una comunicación de correo, es especialmente útil para ofrecer protección a los protocolos de correo normalmente inseguros.

El programa `stunnel` utiliza bibliotecas SSL externas (como las bibliotecas OpenSSL incluidas en Red Hat Linux) para ofrecer un cifrado eficaz y proteger las conexiones. Puede solicitar a una *Autoridad de certificados (CA)* un certificado SSL o crear un certificado firmado propio para obtener las ventajas de un comunicación cifrada con SSL.

Para crear un cifrado SSL con firma propia, cambie al directorio `/usr/share/ssl/certs`, escriba el comando `make stunnel.pem` y responda a las preguntas. A continuación, use `stunnel` para arrancar el demonio de correo que desee usar.

Por ejemplo, se puede utilizar el siguiente comando para iniciar el servidor IMAP incluido en Red Hat Linux:

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/imapd
imapd
```

Ahora podrá abrir un cliente de correo IMAP y conectar al servidor de correo utilizando cifrado SSL. Por supuesto, probablemente desee avanzar más y configurar el servidor IMAP con ajuste de `stunnel` para arrancar automáticamente en los niveles de ejecución correctos.

Para obtener más información sobre cómo usar `stunnel`, lea la página de man de `stunnel` o consulte los documentos del directorio `/usr/share/doc/stunnel-<version-number>`.

Como alternativa, el paquete `imap` incluido en Red Hat Linux contiene una función que proporciona cifrado SSL sin `stunnel`. Para disponer de conexiones IMAP seguras, cree el certificado SSL cambiando al directorio `/usr/share/ssl/certs` y ejecutando el comando `make imapd.pem`. A continuación, defina el servicio `imapd` para que arranque en los niveles de ejecución correctos.

También puede usar el paquete `ipop3` de Red Hat Linux para proporcionar cifrado SSL sin `stunnel`.

15.7. Recursos adicionales

Muchos usuarios consideran al principio muy difícil configurar los programas de correo, principalmente por la gran cantidad de opciones disponibles. El acceso a documentación adicional puede ser muy útil, especialmente para establecer las opciones de configuración más sensibles.

15.7.1. Documentación instalada

- Se incluye información sobre cómo configurar Sendmail en los paquetes `sendmail` y `sendmail-cf`.
  - `/usr/share/doc/sendmail/README.cf` - Contiene información sobre `m4`, ubicaciones de ficheros de Sendmail, mailers compatibles, información sobre cómo tener acceso a funciones mejoradas y mucho más.
  - `/usr/share/doc/sendmail/README` - Contiene información sobre la estructura de directorios de Sendmail, compatibilidad para el protocolo IDENT, información sobre permisos de directorio y problemas comunes que pueden ocasionar estos permisos si se configuran mal.

  Además, las páginas man de `sendmail` y `aliases` contienen información útil sobre varias opciones de Sendmail y la configuración correcta del fichero `/etc/mail/aliases` de Sendmail, respectivamente.
- `/usr/share/doc/fetchmail-<version-number>` - Contiene una lista completa de las funciones de Fetchmail en el fichero `FEATURES` y el documento básico `FAQ`.
- `/usr/share/doc/procmail-<version-number>` - Contiene el fichero `README` con una descripción general de Procmail, el fichero `FEATURES` que analiza las funciones del programa y el fichero `FAQ` con respuestas a distintas preguntas de configuración frecuentes.

  Para obtener información sobre cómo funciona Procmail y cómo se crean recetas, no olvide consultar las siguientes páginas man de Procmail:
  - `procmail` - Proporciona una descripción sobre el funcionamiento de Procmail y los pasos relacionados con filtrar el correo electrónico.
  - `procmailrc` - Explica el formato del fichero `rc` que se usa para crear recetas.
  - `procmailex` - Ofrece un número de ejemplos reales y útiles de recetas de Procmail.
  - `procmailsc` - Explica la técnica de evaluación ponderada que Procmail usa para ver si una receta concreta coincide con un mensaje determinado.

15.7.2. Sitios Web útiles

- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-Administrator-HOWTO.html - Proporciona una descripción general sobre el funcionamiento del correo electrónico, y examina soluciones y configuraciones de correo electrónico en el cliente y en el servidor.
- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-User-HOWTO - Analiza el correo electrónico desde la perspectiva del usuario, evalúa varios programas cliente de correo muy conocidos y ofrece una introducción a temas como alias, reenvío, autorespuesta, listas de distribución, filtros de correo y correo basura.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Secure-POP+SSH.html - Muestra un modo de recuperar correo POP utilizando SSH con reenvío de puerto para que las contraseñas y los mensajes de correo electrónico se transfieran de forma segura.
- http://www.sendmail.net - Contiene noticias, entrevistas y artículos sobre Sendmail, incluida una visión ampliada de las muchas opciones disponibles.
- http://www.sendmail.org - Ofrece una descripción analítica y técnica detallada sobre las funciones de Sendmail. También incluye ejemplos de configuración.
- http://tuxedo.org/~esr/fetchmail - Página principal de Fetchmail que contiene un manual en línea y un apartado FAQ muy completo.

- http://www.procmail.org - Página principal de Procmail con enlaces a listas de distribución dedicadas a Procmail y a varios documentos FAQ.
- http://www.ling.helsinki.fi/users/reriksso/procmail/mini-faq.html - Sección FAQ excelente sobre Procmail con sugerencias para solucionar problemas, e información sobre el bloqueo de ficheros y el uso de caracteres comodín.
- http://www.uwasa.fi/~ts/info/proctips.html - Miles de sugerencias que facilitan el uso de Procmail en distintas situaciones, incluido cómo probar los ficheros `.procmailrc` y cómo utilizar la valoración de Procmail para decidir si se debe adoptar una acción concreta.

15.7.3. Libros relacionados

- *Sendmail* de Bryan Costales con Eric Allman y al; O'Reilly & Associates - Excelente referencia sobre Sendmail redactada con la ayuda del creador original de Delivermail and Sendmail.
- *Removing the Spam: Email Processing and Filtering* de Geoff Mulligan; Addison-Wesley Publishing Company - Volumen que analiza los distintos métodos usados por los administradores de correo que utilizan determinadas herramientas, como Sendmail y Procmail, para gestionar problemas de correo basura.
- *Internet Email Protocols: A Developer's Guide* de Kevin Johnson; Addison-Wesley Publishing Company - Proporciona un análisis muy exhaustivo de los principales protocolos de correo y la seguridad que proporcionan.
- *Managing IMAP* de Dianna Mullet y Kevin Mullet; O'Reilly & Associates - Describe los pasos necesarios para configurar un servidor IMAP.

Capítulo 16.

Berkeley Internet Name Domain (BIND)

Actualmente, Internet y todas las redes locales dependen de un *Servicio de nombres de dominio(Domain Name Service, DNS)* eficaz y fiable que se usa para asociar los nombres de sistemas a las direcciones IP y viceversa.

Para poder obtener un DNS en la red, se necesita un *servidor de nombres* el cual traduce las direcciones IP necesarias para sus resoectvas conexiones. Además, un servidor de nombres puede efectuar la traducción en el nombre del sistema, lo que se llama a menudo *reverse lookup*, o resolución inversa.

Este capítulo describe BIND, la estructura de sus ficheros de configuración y la manera en la que se puede administrar localmente o a distancia.

Para mayor informacio´n sobre la configuración de BIND usando la herramienta gráfica **Herramienta de configuración de Bind** (`redhat-config-bind`), lea el capítuloco llamado *Configuracion de BIND* en el *Manual oficial de personalización de Red Hat Linux*.

Advertencia

Si usa **Herramienta de configuración de Bind**, no debería modificar de forma manual ningún fichero de configuracion de BIND porque todos los cambios serán sobreescritos la proxima vez que use **Herramienta de configuración de Bind**.

16.1. Introduccio´n al DNS y a BIND

Los sistemas que usan las redes IP tienen que conocer la dirección IP de una máquina para poder conectarse. La mayor parte de los usuarios prefieren usar nombres de máquinas como el nombre de un host o de un *fully qualified domain name (FQDN)*, para especificar el sistema en el momento de la conexión.

El uso de nombres de un dominio completamente cualificado tiene ventajas para los administradores del sistema. éstos dan a los administradores flexibilidad a la hora de cambiar las direcciones IP para máquinas individuales sin realizar preguntas sobre el nombre en las máquinas. Lós administradóres pueden mezclar las máquinas basadas en nombre de un modo transparente para el usuario.

El servicio que lo facilita causa DNS y normalmente se implementa mediante el uso de servidores centralizados que autorizan algunos dominios y se refieren a otros servidores DNS para otros dominios.

DNS a través de Linux es posible mediante el uso de un demonio *nameserver* que ejecuta la traducción de IP/hostname. Una aplicación de cliente pedirá información desde el nombre del servidor, habitualmente conectándolo en el puerto 53 del servidor. El nombre del servidor intentará resolver el FQDN basado en su librería de resolución, que puede contener la información de autorización sobre el host necesario o los datos de la caché sobre el nombre. Si el nombre de servidor no posee la pregunta en su librería de resolución, volverá a otros nombres de servidores, llamados *nombres de servidor de root*, para determinar que nombres de servidores autorizados para el FQDN en cuestión. Con esa información, pedirá los nombres de servidor autorizados para ese nombre para determinar la dirección IP. Si ejecuta una búsqueda inversa, se usará el mismo procedimiento, excepto si la pregunta se hace en una dirección IP desconocida más que un nombre.

16.1.1. Zonas

En Internet, el FQDN de un host se puede analizar en diversas secciones y estas secciones se analizan a su vez por orden jerárquico, como en un árbol el tronco, las ramas primarias, las ramas secundarias, etc. Por ejemplo:

```
bill.sales.domain.com
```

Cuando miramos un FQDN para encontrar la dirección IP de un determinado sistema, hay que leer el nombre de derecha a izquierda; los niveles jerárquicos están separados por un punto `.`). En nuestro ejemplo, `com` define el *dominio superior* para este FQDN. El nombre del `domain` es un subdominio de `com`, con `sales` como subdominio de `domain`. El nombre que se encuentra más a la derecha es un FQDN de un host que identifica una determinada máquina.

Aparte del nombre del dominio, cada sección se llama *zona*, la cual define un espacio de nombre particular (namespace). Un *namespace*, o espacio de nombre, controla los nombres de los subdominios de la izquierda. Aunque en el ejemplo solamente hay dos subdominios, un FQDN tiene que contener al menos un subdominio pero puede incluir muchos más; depende de la organización del espacio de nombres elegido.

Las zonas las defienen servidores de nombres que hacen de autoridad con la utilización de *ficheros de zona*, que describen el espacio de nombres de esa zona, los servidores de correo que un determinado subdomnio tiene que usar. Los ficheros de zona se almacenan en los *servidores de nombres primarios*) ,que son los que tienen la autoridad y donde se realizan los cambios de los ficheros, y en los *servidores de nombres esclavos* (que se llaman también *servidores de nombres secundarios*), que reciben los ficheros de zona de los servidores de nombres maestros o primarios. Todos los servidores de nombres pueden ser maestros o esclavos para cada una de las diferentes zonas al mismo tiempo. Todo depende de la configuración de cada servidor de nombres.

16.1.2. Tipos de servidores de nombres

Existen cuatro tipos de servidores de nombres:

- *Maestros* — Almacena los registros de las zonas originales y tienen la autoridad de un cierto espacio de nombres donde buscan respuestas concernientes a dicho espacio de nombres.
- *Esclavo* — Responde también a las peticiones que provienen de otros servidores de nombres y que se refieren a los espacios de nombres sobre los que tiene autoridad. Los servidores esclavos obtienen la información de espacios de nombres de servidores de nombres maestros a través de una *zona de transferencia*, en la que el esclavo manda al servidor maestro un petición que se llama `NoTIFY` para una determinada zona y el maestro responde csi el esclavo está autorizado para recibir la tranferencia.
- *Sólo caché* — ofrece servicios de resolución de nombres a direcciones IP pero no tiene ninguna autoridad sobre ninguna zona. Las respuestas en general se introducen en un caché que se encuentra en la base de datos almacenada en la memoria durante un periodo fijo, la cual está especificada por la zona importada y así obtener una resolución más rápida para otros clientes DNS después de la primera resolución.
- *Posterior* — Hace que determinados servidores de nombres llevan a cabo la resolución. Si alguno de estos servidores no puede efectuar la resolución, el proceso se para y la resolución se anula.

Un servidor de nombres puede ser de varios tipos. Por ejemplo, puede ser servidor de nombres maestro para determinadas zonas, esclavo para otras o incluso ofrecer solamente la transmisión de una resolución.

16.1.3. BIND como servidor de nombres

Red Hat Linux incluye BIND, que es un servidor de nombres open source potente y muy famoso. BIND utiliza el demonio `named` para los servicios de resolución de nombres.

La versión 9 de BIND incluye una utilidad que se llama `/usr/sbin/rndc` y que permite la administración del demonio `named`. Para mayor informacio´n, sobre el comando consulte la Sección 16.3.

16.2. Ficheros de configuración BIND

La configuración del servidor `named` del servidor de nombres BIND es `named` es `/etc/named.conf`. Todos los ficheros de zona están ubicados en el directorio `/var/named/`.

El fichero `/etc/named.conf` debe estar libre de errores para que `named` inicie. Mientras que algunas opciones erróneas no se consideran suficientemente críticas para parar el servidor, cualquier error en los argumnetos evitará que el servicio `named` arranque.

Advertencia

No modifique manualmente el fichero `/etc/named.conf` o cualquier otro fichero del `/var/named` si está usando la **>Herramienta de configuración de Bind**. Todos los cambios que se realicen manualmente en este fichero o en cualquier otros fichero de éste, se borrarán cuando se use la próxima vez la herramienta **Herramienta de configuración de Bind**.

16.2.1. `/etc/named.conf`

El fichero `/etc/named.conf` es un conjunto de declaraciones que usa las opciones que se encuentran en los corchetes `{ }`. He aquí cómo está organizado un fichero `/etc/named.conf`:

```
<statement-1> ["<statement-1-name>"] [<statement-1-class>] {
   <computeroutput-1>;
   <computeroutput-2>;
   <computeroutput-N>;
};

<statement-2> ["<statement-2-name>"] [<statement-2-class>] {
   <computeroutput-1>;
   <computeroutput-2>;
   <computeroutput-N>;
};

<statement-N> ["<statement-N-name>"] [<statement-N-class>] {
   <computeroutput-1>;
   <computeroutput-2>;
   <computeroutput-N>;
};
```

<statement-N-name> tan sólo es necesario con `acl`, `include`, `server`, `view` y `zone` statements. *<statement-N-class>* tan sólo se especifica con el argumento `zone`.

A continuación una lista de comentarios válidos que usará en `/etc/named.conf`:

- `//` — Utilice esta línea al inicio del comentario de línea.
- `#` — Utilice esta línea al inicio del comentario de línea.

- `/*` y `*/` — Incluya el texto en estas preguntas para crear un comentario de bloque.
- Los comentarios serán ubicados en `/etc/named` con los caracteres en estilo C `/* */` o detrás de caracteres `//` y `#`.

Los siguientes argumentos se usarán en `/etc/named.conf`:

- `acl <acl-name>4` — Configura una lista de control de acceso de las direcciones IP que permiten o no ciertos servicios `named`. La mayoría del tiempo, las direcciones IP individuales o la anotación de red IP (como por ejemplo `10.0.1.0/24`) se usa para identificar las direcciones IP exactas.

  Algunas listas de control de acceso están definidas, de manera que no tenga que configurar una pauta `acl` para definirlos:

  - `any` — Hace concordar dirección IP.
  - `localhost` — Concuerda cualquier dirección IP que se use el sistema local.
  - `localnets` — Coordina cualquier dirección IP en cualquier red en la que el sistema local está conectado.
  - `none` — No concuerda ninguan dirección IP.

  Cuando lo utilice con otras pautas `/etc/named.conf` y sus opciones, las pautas `acl` pueden ser muy útiles al asegurar el uso correcto de su servidor de nombre BIND como en el ejemplo:

```
  acl black-hats {
    10.0.2.0/24;
    192.168.0.0/24;
 };

 acl red-hats {
    10.0.1.0/24;
 };

 computeroutputs {
blackhole { black-hats; };
    allow-query { red-hats; };
    allow-recursion { red-hats; };
 }
```

  `named.conf` contiene dos listas de control de acceso (`black-hats` y `red-hats`.

- `controls` — Configura diversas restricciones de seguridad necesarias para la utilización del comando `rndc` y así poder usar el demonio `named`.

  Consulte la Sección 16.3.1.1 para mayor información sobre la declaración `controls`.

- `include "<file-name>"` — Incluye el fichero especificado en el fichero de configuración que se está usando y que permite así situar los datos de configuración sensibles (como `keys`) en un fichero separado con los permiso que impiden a los usuarios sin privilegios leerlos.
- `key "<key-name>"` — Define una clave particular. Estas claves sirven para autenticar dversas acciones como la actualización de la seguridad o la utilización del comando `rndc`. Se usan dos opciones con `key`:

  - `algorithm <algorithm-name>` — El tipo de algoritmo utilizado, como `dsa` o `hmac-md5`.
  - `secret "<key-value>"` — La clave encriptada.

  Consulte Sección 16.3.1.2 para recibir instrucciones sobre como escribir una declaración `key`. `key`.

- `logging` — Permite usar varios tipos de logs que se llaman *channels o canales*. Usando la opción `channel` en la declaración `logging`, se puede construr un tipo de log personalizado con el nombre del fichero (`file`), con el tamaño(`size`), la versión (`version`) y el nivel de importancia

(`severity`. Una vez que se ha definido el canal personalizado, se usa la opción `category` para calificar el canal y comenzar la conexión mientras que se arranca `named`.

Por defecto, `named` envía mensajes de log a los estándares del demonio `syslog`, que les sitúa en `/var/log/messages` por defecto. Esto se debe a que varios canales estándares se encuentran en BIND junto con varios niveles de importancia como el que trata los mensajes de registros informativos (`default_syslog`) y otro que trata específicamente la correccio n de errores (`default_debug`). La categoría predeterminada `default`, utiliza los canales de BIND para llevar a cabo la conexio n normal sin ninguna configuracio n especial.

La personalizacio n del proceso de conexio n es un proceso que requiere una explicacio n muy detallada y no es el objetivo de este capítulo. Para mayor informacio n, consulte el *Manual de referencia del administrador de BIND 9*.

- `computeroutputs` — asigna valores a muchas opciones entrelazadas, incluidos los comandos que se usan para situar un fichero de funcionamiento de `named`, el nombre de ficheros y otros.

  Las siguientes opciones son las más utilizadas:

  - `allow-query` — Especifica lo s ho sts que se usarán para establecer las peticio nes en el servido r de no mbres. Po r defecto , to do s lo s ho sts están auto rizao do s a presentar peticio nes. Se puede usar una lista de co ntro l de acceso o una co lección de direccio nes IP para no auto rizar a un determiando número de servido res de no mbres.
  - `allow-recursion` — Parecida a la o pción `allow-query`, salvo que se aplica a las peticio nes recursivas. Po r defecto , to do s lo s ho sts están auto rizado s a presentar peticio nes en eu servido r de no mbres.
  - `directory` — Reemplaza el fichero de funcio namiento de `named` en vez del fichero predeterminado `/var/named`.
  - `forward` — Co ntro la cómo se lleva a cabo el fo rwarding, si la o pción `forwarders` co ntiene direccio nes IP válidas que designen dónde enviar las peticio nes.

    Si se usa la o pción `first`, lo s servido res de no mbres esecificado s en la o pción `forwarders` so n lo s primero s en recibir las peticio nes y si no pueden so lucio narlas el demo nio `named` intenta la reso lución.

    Si se usa la o pción `only`, `named` no intentará la reso lución si lo s servido res de no mbres han fallado .
  - `forwarders` — Especifica una lista de servido res de no mbres a lo s que hay que mandar las peticio nes para o btener la reso lución.
  - `listen-on` — Especifica el dispo sitivo de red que `named` va a utilizar para recibir las peticio nes. Po r defecto m se usan to do s lo s dispo sitivo s.

    Esta o pción es útil si dispo ne de más de un dispo sitivo de red y desea limitar lo s sistemas que puedan efectuar las peticio nes gateway y servido r de no mbres y desea blo quear to das las peticio nes excepto las que pro vienen de su red privada, la o pción en su servido r `listen-on` será parecida a:

    ```
    options {
      listen-on { 10.0.1.1; };
    };
    ```

    De esta manera, so lamente se aceptan las peticio nes que pro vienen del dispo sitivo de red de la red privada (`10.0.1.1`).
  - `notify` — Determina si `named` envía no tificacio nes a lo s servido res esclavo s cuando una zo na se actualiza. Po r defecto , se usa la o pción `yes`, pero se puede usar también la o pción `no`, para evitar que se manden no tificacio nes a lo s servido res esclavo y así so lamente mandar las no tificacio nes a lo s servido res de la lista `also-notify`.
  - `pid-file` — Permite especificar la lo calización del fichero del pro ceso ID creado po r `named` cuando arranca.

- `statistics-file` — Permite especificar la lo calización del fichero de estadística que se ha creado . Po r defecto , las estadísticas de `named` se encuentran en `/var/named/named.stats`.

Existen numero sas o pcio nes dispo nibles, muchas de ellas dependen unas de o tras para po der funcio nar co rrectamente. Co nsulte el *Manual de referencia del administrado r BIND 9* para mayo r info rmación.

- `server` — Define o pcio nes particulares que afectan a la manera en la que `named` reaccio na ante lo s servido res de no mbres distantes y particularmente co nciernen a las no tificacio nes y las transferencias de zo na.

  La o pción `transfer-format` determina si se ha enviado el reco rd de lo s recurso s co n cada mensaje (`one-answer`) o la grabación de recurso s múltiples co n cada mensaje (`many-answers`). Aunque la o pción `many-answers` es más eficaz, so lamente lo s último s servido res de no mbres BIND la entienden.

- `trusted-keys` — Co ntiene las calves públicas que usa DNSSEC. Para mayo r info rmación so bre la seguridad de BIND, co nsulte la Sección 16.4.3.

- `view "<view-name>"` — Visualizacio nes especiales que respo nden a un tipo de info rmación particular dependiendo del ho st que co ntacta el servido r de no mbres. Esto permite a determinado s ho sts recibi una respuesta que se refiere a una zo na particular mientras que o tro s ho sts reciben info rmación co mpletamente diferente. Alternativamente, cierto s ho sts pueden estar auto rizado s para acceder a determinadas zo nas mientra que o tro s meno s auto rizado s co ntinuan a efectuar peticio nes a o tro s zo nas.

  Se pueden usar múltiples visualizacio nes, las cuales tienen un so lo no mbre. La o pción `match-clients` especifica las direccio nes IP que se aplican a una visualización determinada. Se pueden usar to das las declaracio nes `computeroutput` en un a visualizaci&óacute;n, aunque tienen prioridad las opciones globales ya configuradas para `named`. La mayor parte de las declaraciones `view` contienen múltiples declaraciones `zone` que se aplican a la lista `match-clients`. El orden de aparición en la lista de las declaraciones `view` es importante porque la primera declaración `view` corresponde a la dirección IP de un cliente particular.

  Consulte la Sección 16.4.2 para mayor información sobre la declaración `view`.

- `zone "<zone-name>"` — Especifica zonas particulares para las que está autorizado es servidor de nombres. La declaración `zone` se usa sobre todo para especificar el fichero que contiene la configuración de la zona y transmite ciertas opciones de esa zona a `named` que tendrán prioridad sobre todas las otras declaraciones `computeroutput` del fichero `/etc/named.conf`.

  El nombre de la zona es importante porque representa el valor por defecto asignado a la directiva `$ORIGIN` que se usa en el fichero de zona y que está relacionado con los el no-FQDN. Por ejemplo, si estas declaración `zone` define el espacio de nombre para `domain.com`, hay que usar `domain.com` y no *<zone-name>* para que se situe al final de los nombres de los hosts que se usan en ese fichero de zona.

  Las opciones más usadas de la declaración `zone` son las siguientes:

  - `allow-query` — Especifica los clientes que se autorizan para pedir información sobre una zona. Por defecto todas las peticiones de información sin autorizadas.

  - `allow-transfer` — Especifica los servidores esclavos que están autorizados para pedir una transferencia de información de la zona. Por defecto, todas las peticiones se autorizan.

  - `allow-update` — Especifica los hosts que están autorizados para actualizar dinámicamente la informción de la zona. Por defecto, no se autoriza la actualización de la información.

Advertencia

Tenga cuidado cuando autorice a los hosts para actualizar la información de la zona. No habilite esta opción si no tiene confianza en el host que vaya a usar. Es mejor que el administrador actualice manualmente los records de zona y que recargue el servicio `named`, si es posible.

- `file` — Especifica el nombre del fichero que contiene los datos de configuración de la zona en el fichero de funcionamiento `named` (por defecto `/var/named`).
- `masters` — Se utiliza si la zona se define como `type` esclava. La opción `masters` indica al `named` de un esclavo la/las direcciones en las que se puede pedir información de las zona en la que se tiene autoridad.
- `notify` — Es parecida a la opción `notify` que se usa con la declaración `computeroutput`.
- `type` — Define el tipo de zona. Se pueden usar los siguientes tipos:
  - `forward` — Dice al servidor de nombres que lleve a cabo todas las peticiones de información de la zona en cuestión hacia otros servidores de nombres.
  - `hint` — Tipo especial de zona que se usa para orientar hacia los servidores de nombres root que sirven para resolver peticiones de una zona que no se conoce. Normalmente, no tendrá que configurar una zona que está situada fuera del `/etc/named.conf`.
  - `master` — Designa el servidor de nombres actual que tiene la autoridad en esa zona. Una zona se puede configurar como tipo `master` si tiene ficheros de configuración de la zona en el sistema actual.
  - `slave` — Designa el servidor de nombres actual que es servidor esclavo para dicha zona y le dice a `named` que pida los ficheros de configuración de la zona de las direcciones IP al servidor de nombres master.

- `zone-statistics` — Dice a `named` que conserve las estadísticas que conciernen a esa zona escribiéndolas bien en la localización por defecto de (`/var/named/named.stats`), o en la localización designada por la opción `statistics-file` en la declaración `server`, si existe.

16.2.1.1. Ejemplos de declaraciones de zona

La mayor parte de los cambios del fichero `/etc/named.conf` de un servidor de nombres maestro o esclavo se refieren a añdir. modificar o suprimir declaraciones de `zone`. Aunque estas declaraciones pueden contener muchas opciones, la mayor parte de los servidores de nombres usan pocas. Las declaraciones de `zone` siguientes son ejemplos básicos que se pueden usar en una relación de servidores de nombre maestro/esclavo.

A continuación un ejemplo de declaración `zone` para el host del servidor de nombres primario en `domain.com`:

```
zone "domain.com" IN {
  type master;
  file "domain.com.zone";
  allow-update { none; };
};
```

En la declaración, la zona está identificada como `domain.com`, la tipografía está configurada para `maestro` y el servicio `named` está indicado para leer el fichero `/var/named/domain.com.zone`. Hace que `named` no se actualice por ningún otro host.

Una declaración del servidor esclavo para `zone` parece diferente a `domain.com` al ejemplo previo. Para un servidor esclavo, la tipografía está configurada para `slave` y en lugar de la línea `allow-update` encontrará una directiva que le diga la dirección IP de `named` del servidor master.

Una declaración de servidor esclavo para el domain.com será parecida a:

```
zone "domain.com" {
  type slave;
  file "domain.com.zone";
```

```
  masters { 192.168.0.1; };
};
```

Esta declaración de `zone` dice a `named` en el servidor esclavo que busque el servidor maestro `192.168.0.1` para encontrar la información de configuración para la zona `domain.com`. La información que el servidor esclavo recibe se registran en el fichero `/var/named/domain.com.zone`.

16.2.2. Ficheros de zona

Los *ficheros de zona* que contienen información sobre el espacio de nombre particular se almacenan en el fichero de funcionamiento de `named`, que por defecto es `/var/named`. Cada fichero de zona se nombra según los datos de las opciones de `file` en la declaración `zone`, generalmente de tal manera que se refiere al dominio en cuestión e identifica el fichero que contiene los datos de zona como `example.com.zone`.

Cada fichero de zona puede contener directivas y registros de recursos. Las *directivas* dicen al servidor de nombres que efectue una determinada acción o que aplique una configuración especial a la zona. Los *registros de recursos* definen los parámetros de la zona asiganando una identidad a sistemas particulares en el interior del espacio de nombre de la zona. Las directivas no son obligatorias pero los registros de recursos son necesarios para ofrecer un servicio de nombres a dicha zona. Todas las directivas y registros de recursos tienen que estar en la línea correspondiente.

Se pueden escribir comentarios en los ficheros de zona después de los puntos y comas (`;`).

16.2.2.1. Directivas de los ficheros de zona

Las directivas se identifican por el caracter `$` que se sitúa delante del ombre de la directiva y generalmente en la parte de arriba del fichero de zona.

A continuación le mostramos las directivas más usadas:

- `$INCLUDE` — Dice a `named` que incluya otro fichero de zona en el fichero de zona donde se usa la directiva. Así se pueden almacenar configuraciones de zona suplementarias que dependen del fichero de zona principal.
- `$ORIGIN` — Determina el nombre del registro no cualificado, como por ejemplo los que especifican solamente el host.

  Por ejemplo, un fichero de zona puede contener la línea siguiente:
  ```
  $ORIGIN domain.com
  ```

  Todos los nombres que se usan en los registros de recursos y qu eno acaban por un punto (`.`) se añaden al nombre de dominio. Es decir, cuando el servidor lee el registro de zona, la primera línea de arriba se interpretará como segunda línea:
  ```
  ftp               IN   CNAME   server1
  ftp.domain.com.   IN   CNAME   server1.domain.com.
  ```

  Nota

  La utilizacion de la directiva `$ORIGIN` no es necesaria si nombramos la zona en `/etc/named.conf` con el valor de la opción `$ORIGIN`. El nombre de la zona se usa por defecto como valor de la directiva `$ORIGIN`.

- `$TTL` — Ajusta el valor *Time to Live (TTL)* predeterminado para la zona. Es el nombre, en segundos, que se da a los servidores de nombres para determinar cuánto tiempo los registros de recursos

de la zona serán válidos. Un registro de recursos puede contener su propio valor TTL, que tendrá prioridad sobre la directiva presente.

Cuando se decide aumentar este valor la esta directiva dice a los servidores de nombres que metan en caché esta información de zona durante máa tiempo. Esto reduce el número de peticiones de la zona pero aumenta el tiempo necesario para aumentar la cantidad de registros de recursos.

16.2.2.2. Registros de recursos de ficheros de zona

Los regisitros de recursos de ficheros de zona contienen columnas de datos, separadas por un espacio, que definen estos registros. Todos los registros de recursos de ficheros de zona están asociados a un tipo particular que designa el motivo del registro. A continuación le mostramos los tipos de registros más frecuentes:

- `A` — Registro de dirección que especifica una dirección IP que se debe asignar a un nombre, como en el ejemplo:

```
<host>      IN      A      <IP-address>
```

  Si se omite el valor *<host>*, el registro `A` designa una dirección IP predeterminada para la parte superior del nombre. Este sistema es la base de todas las peticiones que no sean FQDN.

  Consideremos los siguiente ejemplos del registro `A` para el fichero de la zona `domain.com`:

```
             IN      A       10.0.1.3
server1      IN      A       10.0.1.5
```

  Las peticiones para el dominio `domain.com` se dirigen al valor 10.0.1.3, mientra que las del dominio `server1.domain.com` se dirigen al valor 10.0.1.5.

- `CNAME` — Registro del nombre canónico, que enlaza un nombre con otro: un alias.

  El siguiente ejemplo le dice a `named` que cualquier petición enviada a *<alias-name>* señalará el host, *<real-name>*. Los registros `CNAME` que usan un esquema de nombres comunes en el host correcto.

```
<alias-name>      IN      CNAME       <real-name>
```

  Examinemos el siguiente ejemplo. En esta configuración un registro `A` liga un nombre de host a una dirección IP, mientras que el registro `CNAME` señala el nombre del host más utilizado `www`.

```
server1      IN      A       10.0.1.5
www          IN      CNAME   server1
```

- `MX` — Registro Mail eXchange, que dice dónde se tiene que dirigir el correo enviado a un nombre de espacio particular controlado para esa zona.

```
      IN      MX      <preference-value>   <email-server-name>
```

  La opción *<preference-value>* le permite listar numéricamente los servidores de correo que seleccione para recibir mensajes para ese espacio de nombres, dando preferencia a ciertos sistemas de correo. El registro de recursos `MX` tiene el valor más bajo de la opción *<preference-value>*,pero puede ajustar varios servidores de correo con el mismo valor para distribuir el tráfico de correo entre ellos.

  La opción*<email-server-name>* puede ser un nombre de host o un FQDN, siempre y cuando se oriente hacia el sistema adecuado.

```
      IN      MX      10      mail.domain.com.
      IN      MX      20      mail2.domain.com.
```

  En este ejemplo, el primer servidor de correo `mail.domain.com` se prefiere al servidor `mail2.domain.com` para recibir los correos destinados al dominio `domain.com`.

- NS — egistro de servidor de nombres (NameServer) que indica a los servidores los servidores de nombres que tienen la autoridad de una determinada zona.

  éste es un ejemplo del registro NS:

  ```
  IN     NS     <nameserver-name>
  ```

  La opción <*nameserver-name*> tiene que ser un FQDN.

  A continuación, dos nombres de servidores están listados como autorizados para el dominio. No es importante si estos servidores de nombre son esclavos o no o si uno es maestro, ambos son considerados como autorizados.

  ```
  IN     NS     dns1.domain.com.
  IN     NS     dns2.domain.com.
  ```

- PTR — Registro PoinTeR creado para orientar hacia otra parte del espacio de nombres.

  Los registros PTR sirven, sobre todo,para la resolución inversa de nombres ya que reorientan las direcciones IP hacia un mobre determinado. Consulte la Sección 16.2.2.4 para ver maás ejemplos de esta opción.

- SOA — Registro "Start Of Authority", que proclama información importante sobre la autoridad de determinados servidores sobre determinados espacios de nombres.

  Está situado detrás de las directivas y es el primer registro en un fichero de zona.

  El siguiente ejemplo muestra la estructura básica de un registro SOA:

  ```
  @      IN     SOA    <primary-name-server>      <hostmaster-email> (
                       <serial-number>
                       <time-to-refresh>
        <time-to-retry>
        <time-to-expire>
        <minimum-TTL> )
  ```

  El símbolo @ sitúa la directiva $ORIGIN (o el nombre de zona, si la directiva $ORIGIN no está instalada) mientras que el espacio de nombre esta7aacute; definido por el registro presente de recursos SOA. El servidor de nombres primario que tiene la autoridad para este dominio la usa la opció <*primary-name-server*>, y la dirección de correo electrónico de la persona con la que hay que contactar se reemplaza con <*hostmaster-email*>.

  La opción <*serial-number*> aumenta cada vez que cambia el fichero de zona con el fin de que named sepa que debe recargar esta zona. <*time-to-refresh*> dice a todos los servidores esclavos cuánto tiempo tienen que esperar antes de pedir información al servidor de nombres maestro si se han realizado cambios en la zona. El valor <*serial-number*> lo utiliza el servidor esclavo para determinar si está usando datos caducados o si tiene que actualizarlos.

  La opción <*time-to-retry*> informa al servidor de nombres esclavo sobre el intervalo de tiempo que teiene que esperar antes de emitir una petición de actualización de datos en caso de que el servidor de nombres maestro no le responda. Si el servidor maestro no ha respondido a una petición de actualización de datos antes que se acabe el intervalo de tiempo <*time-to-expire*>, reponde el servidor esclavo presentándose como servidor con la autoridad en este espacio de nombres.

  La opción <*minimum-TTL*> pide a los otros servidores de nombres que situen en caché la información de esa zona durante al menos ese periodo.

  En BIND, el tiempo se mide en segundos. Sin embargo, puede usar las abreviaciones de las otras unidades de tiempo como minutos (M), horas (H), días (D), y semanas (W). La Tabla 16-1 le muestra la cantidad de teiempo en segundos y el periodo equivalente en otro formato.

Segundos	otras unidades de tiempo.
Segundos	otras unidades de tiempo.
60	1M
1800	30M
3600	1H
10800	3H
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W

Tabla 16-1. Equivalencia en segundos de las otras unidades de tiempo

The following example illustrates the form an SOA resource record might take when it is configured with real values.

El ejemplo siguiente le muestra a qué se parece el registro de recursos básico SOAal configurarlo con valores reales.

```
@     IN     SOA    dns1.domain.com.     hostmaster.domain.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expires after 1 week
                    86400 )    ; minimum TTL of 1 day
```

16.2.2.3. Ejemplos de ficheros de zona

Si obervamos las directivas y los registros de recursos por separado, quizás tengamos algunas dificultades en comprenderlos. Sin embargo, si los estudiamos en su conjunto en un fichero no resulta tan difícil. El siguiente ejemplo muestra un fichero de zona muy básico.

```
$ORIGIN domain.com
$TTL 86400
@     IN     SOA    dns1.domain.com.     hostmaster.domain.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expires after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.domain.com.
      IN     NS     dns2.domain.com.

      IN     MX     10     mail.domain.com.
      IN     MX     20     mail2.domain.com.

             IN     A       10.0.1.5

server1      IN     A       10.0.1.5
server2      IN     A       10.0.1.7
```

```
dns1          IN     A       10.0.1.2
dns2          IN     A       10.0.1.3

ftp           IN     CNAME   server1
mail          IN     CNAME   server1
mail2         IN     CNAME   server2
www           IN     CNAME   server2
```

En este ejemplo se usan las directivas estándar y los valores `SOA`. Se ve que los servidores de nombres que tendrán la autoridad son `dns1.domain.com` y `dns2.domain.com`, que tienen como registros `A` que les conecta respectivamente a `10.0.1.2` y `10.0.1.3`.

Los servidores de correo configuados por los registros `MX` s eorientan hacia los servidores `server1` y `server2` gracias a los registros `CNAME`. Debido a que los nombres de los servidores `server1` y `server2` no acaban con un punto (`.`), el dominio `$ORIGIN` se situa a continuación, extendiendo los dominios `server1.domain.com` y `server2.domain.com`. Gracias a los registros de recursos `A` se peuden determinar las direcciones IP.

Los servicios ftp y de web, disponibles en `ftp.domain.com` y `www.domain.com`, están orientados a máuinas que ofrecen los servicios apropiados para dichos nombres usando el registro `CNAME`.

16.2.2.4. Ficheros de resolución de nombres inversa

Una resolución de nombres inversa sirve para traducir una dirección IP en un espacio de nombres particular en un FQDN. Esto se parece mucho a un fichero de zona estándar, salvo que los registros de recursos `PTR` sirven para relacionar las direcciones IP con los nombres de un sistema determinado.

La escritura de un registro `PTR` se hace de la siguiente manera:

```
<last-IP-digit>       IN     PTR    <FQDN-of-system>
```

<last-IP-digit> hace referencia al último nombre en una dirección IP que tiene que orientar el FQDN de un determinado sistema.

En el siguiente ejemplo, las direcciones IP de `10.0.1.20` a `10.0.1.25` se orientan a los FQDNs correspondientes.

```
$ORIGIN 1.0.10.in-addr.arpa
$TTL 86400
@     IN     SOA    dns1.domain.com.     hostmaster.domain.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.domain.com.
      IN     NS     dns2.domain.com.

20    IN     PTR    alice.domain.com.
21    IN     PTR    betty.domain.com.
22    IN     PTR    charlie.domain.com.
23    IN     PTR    doug.domain.com.
24    IN     PTR    ernest.domain.com.
25    IN     PTR    fanny.domain.com.
```

Este fichero de zona se tiene que poner en funcionamiento con una declaración `zone` en el fichero `/etc/named.conf`, parecido a:

```
zone "1.0.10.in-addr.arpa" IN {
  type master;
  file "domain.com.rr.zone";
  allow-update { none; };
};
```

Existe algunas pequeñas diferencias ente este ejemplo y una declaración `zone` estándar, salvo en la manera de nombrar el host. observe que uns zona de resolución de nombres inversa necesita que los tres primeros bloques de la dirección IP sean invertidos y que "`.in-addr.arpa`" esté a su vez incluido. Esto permite asociar correctamente a la zona el bloque único de nombres que se usa en el fichero de zona de resolución de nombres inversa.

16.3. Utilización del comando `rndc`

BIND incluye la utilidad `rndc`, que permite admnistrar localmente o a distancia, el demonio `named` gracias a las declaraciones de las líneas de comandos. El programa `rndc` utiliza el fichero `/etc/rndc.conf` para las opciones de configuración que serán sobrescritas por las opciones de las líneas de comandos.

Para evitar que los usuarios no autorizados a controlar BIND en su sitema, se utiliza el método de claves secretas compartidas para dar privilegios a determinados hosts. Para que `rndc` emita comandos hacia cualquier `named`, incluso hacia la máquina local, las claves utilizadas en los ficheros `/etc/named.conf` y `/etc/rndc.conf` se tienen que corresponder.

16.3.1. Configuración de `rndc`

Antes de usar el comando `rndc`, verifique que las líneas de configuración adecuadas se encuentren en un los ficheros necesarios. Es probable que los ficheros de configuración no estén instalados como debería ser si después de que lanza el comando aparece el siguiente mensaje `rndc`:

```
rndc: connect: connection refused
```

16.3.1.1. `/etc/named.conf` y `/etc/named.conf</`

Para que el comando `rndc` se pueda conectar al servicio `named`, tiene que tener una declaración `controls` en el fichero `/etc/named.conf` cuando arranque `named`. El ejemplo de declaración `controls` le permite ejecutar los comandos `rndc` localmente.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Esta declaracoón dic a `named` que tiene que escuchar en el puerto TCP 953 por defecto de la dirección inversa y que tiene que autorizar los comandos `rndc` que provienen del host local, si existe la clave adecuada. <*key-name*> hace referencia a la declaración `key`, que también se encuentra en el fichero `/etc/named.conf`. Puede ver un ejemplo de este tipo de declaración.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

En este caso, <*key-value*> es una clave HMAC-MD5. Puede crear sus propias claves HMAC-MD5 con el siguente comando.

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

Una calve de al menos 256 bits de longitud es una buena elección. La clave creada tiene que situarse en la zona <*key-value*> que se encuentra en <*key-file-name*>.

El nombre de la clave utilizada en `/etc/named.conf` tiene que ser diferente de `key`.

16.3.1.2. `/etc/rndc.conf`

Necesita añadir las siguientes líneas para `/etc/rndc.conf` si `rndc` usa de forma automática la claves específicas `/etc/named.conf`. Esto se hace mediante la declaración `options` statement:

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Este comando configura una clave predeterminada general, pero el comando `rndc` puede usar claves diferentes para servidores particulares, como en el siguiente ejemplo:

```
server localhost {
  key  "<key-name>";
};
```

Sin embargo, esta declaración `server` es realmente útil si se quiere conectar a varios servidores con el comando `rndc`.

La declaración `key` es la más importante del fichero `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

<*key-name*> y <*key-value*> tienen que ser completamente iguales a la configuración en el fichero `/etc/named.conf`.

Para probar todas las configuraciones, pruebe el comando `rndc reload`. Verá algo parecido a lo siguiente:

```
rndc: reload command successful
```

Si el comando no funciona, examine los ficheros `/etc/named.conf` y `/etc/rndc.conf` para buscar los errores.

16.3.2. opciones de la línea de comandos `irndc`

Un comando `rndc` tiene la siguiente forma:

```
rndc <options> <command> <command-options>
```

La zona <*options*> o es necesaria y no debe usar <*command-options*> a menos que el comando lo necesite.

Cuando ejecuta el comando `rndc` en un host local, se encuentran disponibles los siguientes comandos:

- `halt` — Para inmediatamente el servicio `named`.
- `querylog` — Ejecuta la conexión para todas las peticiones efectuadas por los clientes hacia el servidor de nombres.
- `refresh` — Actualiza la base de datos del servidor de nombres.
- `reload` — Dice al servidor de nombres que recargue los ficheros de zona paro que conserve todas las respuestas precedentes situadas en caché. Esto le permite realizar cambios en los ficheros de zona y de ponerlos en práctica en los servidores maestros y esclavos sin perder las resoluciones de nombres almacenadas.

  Si los cambios no afectan a una zona determinada, puede decir al comando `named` que recargue esa zona. Escriba el nombre de la zona después del comando `reload`.
- `stats` — Pasa las estadísticas del comando `named` al fiochero `/var/named/named.stats`.
- `stop` — Para el servidor salvando todas las actualizaciones dinámicas y los datos IXFR antes de parar el servidor completamente.

Se pueden sobrescribir los parámetros predeterminados del fichero `/etc/rndc.conf`. Existen varias posiblidades:

- `-c <configuration-file>` — Dice al comamdo t à `rndc` que use otro fichero de configuración diferente del fichero predeterminado `/etc/rndc.conf`.
- `-p <port-number>` — Especifica la utilización de un número de puerto diferente del predeterminado 953 para la conexión del comando `rndc`.
- `-s <server>` — Dice a `rndc` que envie comandos a otro servidor distinto del servidor que designa la opción `default-server` en el fichero `/etc/rndc.conf`.

  Para que se lleve a cabo esta tarea, tiene que aver configurado el servicio `named` para que acepte los comandos del host y que tenga la clave para este servicio de nombres.
- `-y <key-name>` — Le permite especificar una clave distinta de la opción `default-key` en el fichero `/etc/rndc.conf`.

Para mayor información sobre estas opciones, consulte la página man del comando `rndc`.

16.4. Propidades avanzadas de BIND

La mayor parte de las acciones de BIND usan `named` solamente para ofrecer un servicio de resolución de nombres o para obtener la autoridad de un dominio o subdominio particular. Sin embargo, la versión 9 de BIND posee un determinado número de propiedades avanzadas que cuando se configuran y se usan de manera adecuada, permiten ofrecer un servicio DNS eficaz y seguro.

Advertencia

Algunas de estas propiedades avanzadas como DNSSEC, TSIG y IXFR, solamente se pueden usar en los entornos de red que tengan servidores de nombres que soporten estas propiedades. Si su entorno de red incluye servidores de nombres no-BIND o versiones anteriores de BIND verifique si la propiedad avanzada está soportada.

No se presupone que otro servidor de nombres soporte estas propiedades porque en general no lo hacen.

Todas las propiedades citadas aquí se describen en el *Manual de referencia del administrador de BIND 9*. Consulte la Sección 16.6 para mayor información.

16.4.1. Mejoras del protocolo DNS

BIND soporta las *Incremental Zone Transfers,(IXFR)*, en las que el servidor de nombres esclavo descarga solamente las porciones de actualizaciones de una zona modificada en un servidor de nombres maestro. El proceso de tranferencia AXFR estándar necesita que la zona entera se transfiera al servidor de nombres esclavo incluso si se hacen pequeños cambios. Para los dominios más famosos con ficheros de zona muy largos, IXFR hace que la notificación y los procesos de actualización sean menos exigentes en recursos.

observe que IXFR solamente estáa disponible si usa al mismo tiempo la *actualización dinámica* para realizar los cambios en los registros de zona maestra. Si cambia los ficheros de zona manualmente para dichos cambios, tiene que usar AXFR. Encontrará más información en el *Manual de referencia del administrador* .

16.4.2. Visualizaciones múltiples

BIND le permite con la opción `view` en `/etc/named.conf`, configurar un servidor de nombres para responder a las peticiones de determinados clientes en una manera diferente de otros.

Esto es útil sobre todo si desea que clientes externos a su red no puedan ejecutar un servicio DNS particular o que accedan a una determinada información , siempre y cuando se autoricen a los clientes internos.

La declaración `view` utiliza la opción `match-clients` para hacer corresponder las direcciones IP o las redes enteras y atribuirlas opciones y datos de zonas específicas.

16.4.3. Seguridad

BIND soporta varios métodos diferentes para proteger la actualización y la transferencia de zonas al mismo tiempo que a los srvidores de nombres maestros y esclavos:

- *DNSSEC* — Abreviación de *DNS SECurity*, esta propiedad permite firmar con caracteres criptográficos zonas con una *clave de zona (zone key)*.

  De esta manera, puede verificar que la información de una zona provenga de un servidor de nombres que la ha firmado con caracteres crptográficos con una clave privada desde el momento en que el receptor posee la clave pública de ese servidor de nombres.

  La versión 9 de BIND soporta también el método de la llave públoca/privada SIG(0) para la autentificación de mensajes.

- *TSIG* — Abreviacioacute;n de *Transaction SIGnatures*, instala una clave secreta compartida en el servidor maestro y el servidor esclavo y verifica que la transferencia del servidor maestro al esclavo esté autorizada.

  Esta propiedad refuerza la autorización de transferencias basada en la dirección IP estándar. Un agresor no puede acceder a la dirección IP para transferir la zona porque necesita conocer la clave secreta.

  La versión 9 de BIND soporta también *TKEY*, que es otro método de clave secreta compartida para autorizar las transferencias de zona.

16.4.4. IP versión 6

La versión 9 de BIND ofrece un servicio de nombres en la versión 6 (IPv6), gracias a los registros de zona `A6`.

Si su entorno de red incluye al mismo tiempo hosts IPv4 y IPv6, necesita usar el demonio de resolución ligero `lwresd` en los clientes de red. Este demonio es muy eficaz y funciona solamente en caché, que soporta los nuevos registros `A6` y `DNAME` que funcionan con IPv6. Consulte la página man `lwresd` para mayor información.

16.5. Errores frecuentes que hay que evitar

Es normal que los principiantes cometan errores modificando los ficheros de configuración BIND o que encuentren dificultades a la hora de activar el comando `named`. Evite los siguientes errores:

- *Asegúrese que aumenta el número de serie cuando modifique un fichero de zona.*

  Si el número de serie no ha aumentado, puede ser que el servidor de nombres maestro posea información nueva y correcta pero que los servidores esclavos no hayan recibido ninguna notificación de los cambios o que no intenten actualizar los datos de esa zona. Después de todo, el número de serie corresponde al que se encuentra en el servidor maestro aunque los datos de esta zona sean completamente diferentes a los del servidor maestro.
- *Preste atención a la utilización de los corchetes y de los puntos y comas en el fichero `/etc/named.conf`.*

  La omisión de un punto y coma o de un corchete impide que arranque `named`.
- *Acuérdese de situar los puntos (`.`) en los ficheros de zona después de los FQDN y de evitarlos en los nombres de hosts.*

  El punto significa que el nombre está completo. Si se omite el punto, `named` situará el nombre de la zona o el valor `$ORIGIN` después del nombre para completarlo.
- *Si el firewall bloquea las conexiones con el comando `named` con otros servidores de nombres, tendrá que modificar el fichero de configuración.*

  Por defecto, la versión BIND usa los puertos aleatorios por encima de 1024 para pedir otros servidores de nombres. Algunos firewalls, sin embargo, esperan todos los servidores de nombres para comunicarse mediante el uso del puerto 53. Puede forzar esta conducta añadiendo la siguiente línea a una declaración `options` en `/etc/named.conf`:

  ```
  query-source address * port 53;
  ```

16.6. Recursos adicionales

Las fuentes de información siguientes le ofrecen documentación adicional sobre la utiliación de BIND.

16.6.1. Documentación instalada

- BIND propone toda una gama de documentación instalada que cubre numerosos aspectos, cada uno se encuentra en un fichero distinto:
  - `/usr/share/doc/bind-<version-number>` — Contiene un fichero `README` con la lista de las propiedades más recientes.

- `/usr/share/doc/bind-<version-number>/arm` — Contiene las versiones en HTML y SGML del *Manual de referncia del administrados BIND 9*, que describe en detalle los recursos necesarios para BIND, la manera de configurar los diferentes tipos de servidores de nombres, cómo establecer un equilibrio de cargas y otros temas de interés. Es el mejor punto de partida para los principiantes.
- `/usr/share/doc/bind-<version-number>/draft` — Contiene los documentos técnicos que se refieren al servicio DNS y a algunos métodos propuestos para responder a las resoluciones.
- `/usr/share/doc/bind-<version-number>/misc` — Contiene documentos para cuestiones avanzadas específicas. Los usuarios de la versión 8 de BIND tendrían que consultar el documento `migration` en lo que se refiere a los cambios importantes cuando se pasa a la versión 9 de BIND. El fichero `computeroutputs` lista todas las opciones disponibles en BIND 9 que se usan en el fichero `/etc/named.conf`.
- `/usr/share/doc/bind-<version-number>/rfc` — Documento RFC sobre BIND.

- Páginas man útiles:
  - `named` — Examina los argumentos que pueden usarse para controlar el demonio del servidor de nombres BIND, como el fichero de configuración alternativo y el funcionamiento en un puerto diferente.
  - `rndc` — Explica las opciones diferentes cuando se usa el comando `rndc` para controlar un servidor de nombres BIND.

16.6.2. Sitios web útiles

- http://www.isc.org/products/BIND — La página del proyecto BIND, donde encontrará información sobre las versiones actuales y las descargas en formato PDF del *Manual de referencia del administrador BIND 9*.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Trata la utilizacio´n de BIND como servidor de nombres de resolución caché y la configuración de diversos ficheros de zon anecesarios en el servidor de nombres maestro para un dominio.

16.6.3. Libros sobre el tema

- *DNS and BIND* por Paul Albitz y Cricket Liu; O'Reilly & Associates — Referencia que explica las opciones de configuración de BIND má sencillas y las más difíciles así como estrategias para asegurar el servidor DNS.
- *The Concise Guide to DNS and BIND* por Nicolai Langfeldt; Que — Estudia la conexión entre los servicios de redes múltiples y BIND, centrándose sobre todo en los aspectos técnicos y orientados a las aplicaciones prácticas.

Capítulo 17.

Network File System (NFS)

NFS (Network File System) permite a máquinas montar particiones en un sistema remoto en concreto y usarlas como si estuvieran en el sistema de ficheros local. Esto permite centralizar ficheros en una localización, mientras se permite su acceso continuo a los usuarios autorizados.

Hay dos versiones de NFS actualmente en uso. La versión 2 de NFS (NFSv2), que tiene varios años, es ampliamente soportada por muchos sistemas operativos. La versión 3 (NFSv3) tiene más características, incluyendo tamaño variable del manejador de ficheros y una mejor información de errores. Red Hat Linux soporta tanto NFSv2 como NFSv3, y usa NFSv3 por defecto cuando se conecta a un servidor que lo soporta.

Este capítulo se centra en la versión 2 de NFS, aunque muchos de los conceptos aquí discutidos también se aplican a la versión 3. Adicionalmente, solo los conceptos fundamentales de NFS e información suplementaria serán proporcionados. Para instrucciones específicas con respecto a la configuración y operación de NFS en servidores o clientes, vea el capítulo titulado *Network File System (NFS)* en el *Manual oficial de personalización de Red Hat Linux.*

17.1. Metodología

Linux usa una combinación de soporte a nivel de kernel y demonios en continua ejecución para proporcionar compartición de ficheros NFS, y el soporte NFS debe estar activo en el kernel de Linux para que funcione. NFS usa *Remote Procedure Calls (RPC)* para enrutar peticiones entre clientes y servidores, implicando que el servicio `portmap` debe estar disponible y activo en los niveles de ejecución adecuados para que la comunicación NFS funcione. Trabajando con `portmap`, varios otros procesos se aseguran que una conexión particular NFS esté permitida y pueda proceder sin error:

- `rpc.mountd` — El proceso que recibe la petición de montaje desde un cliente NFS y chequea para mirar si coincide con un sistema de ficheros actualmente exportado.
- `rpc.nfsd` — El proceso que implementa la parte de usuario del servicio NFS. Trabaja son el kernel Linux para conocer las demandas dinámicas de clientes NFS, tales como proporcionar procesos adicionales del servidor para que los clientes NFS lo utilicen.
- `rpc.lockd` — Un demonio innecesario en los kernels modernos. El bloqueo de de ficheros NFS ahora lo hace el kernel. Está incluido en el paquete `nfs-utils` para usuarios de versiones antiguas del kernel que no incluyen esta capacidad por defecto.
- `rpc.statd` — Implementa el protocolo RPC *Network Status Monitor (NSM)*. Esto proporciona notificación de reinicio cuando un servidor NFS es reiniciado abruptamente.
- `rpc.rquotad` — Un servidor RPC que proporciona información de cuotas de usuarios a usuarios remotos.

No todos estos programas son requeridos para el servicio NFS. Los únicos servicios que deben estar activos son `rpc.mountd`, `rpc.nfsd`, y `portmap`. Los otros demonios proporcionan funcionalidades adicionales y solo deben usarse si el entorno de su servidor los requiere.

La versión 2 de NFS usa el *User Datagram Protocol (UDP)* para proporcionar una conexión de red sin estado entre el cliente y el servidor (la versión 3 de NFS puede usar UDP o TCP corriendo sobre una IP). La conexión UDP sin estado minimiza el tráfico de red, al mandar el servidor NFS una cookie al cliente, después de que el cliente sea autorizado a acceder al volumen compartido. Esta cookie es un valor aleatorio guardado en la parte del servidor y es pasado por cualquier petición RPC del cliente al servidor. El servidor NFS puede ser reiniciado sin afectar a los clientes y las cookies permanecen intactas.

Con NFS, la autentificación solo se produce cuando el cliente intenta montar un sistema de ficheros remoto. Para limitar el acceso, el servidor NFS utiliza en primer lugar divisiones TCP. Estas divisiones leen los ficheros `/etc/hosts.allow` y `/etc/hosts.deny` para determinar si a un cliente particular le debe ser explícitamente permitido o denegado su acceso vía NFS. Para más información sobre cómo configurar los controles de acceso con divisiones TCP, consulte Capítulo 8.

Después de que al cliente se le permitan divisiones TCP pasadas, el servidor NFS recurre a su fichero de configuración, `/etc/exports`, para determinar si el cliente tiene suficientes privilegios para montar alguno de los sistemas de ficheros exportados. Después de permitir el acceso, cualquier operación de ficheros y directorios es mandada al servidor usando llamada de procedimiento remotas.

Aviso

Los privilegios de montajes NFS son permitidos específicamente a clientes, no a usuarios. Si permite a una máquina acceder a un sistema de ficheros exportado, los usuarios de esa máquina podrán acceder a esos datos.

Al configurar el fichero `/etc/exports`, sea extremadamente cuidadoso al otorgar permisos de lectura y escritura (`rw`) a un sistema remoto.

17.1.1. NFS y `portmap`

NFS se apoya en las llamadas de procedimientos remotos (RPC) para funcionar. Se requiere `portmap` para trazar las peticiones RPC a los servicios correctos. Los procesos RPC notifican a `portmap` cuando comienzan, revelando el número de puerto que ellos están monitorizando y el número de programas RPC que esperan servir. El sistema cliente entonces contacta con el `portmap` del servidor con un número de programa RPC particular. Entonces `portmap` redirecciona al cliente al número del puerto apropiado para que se comunique con el servicio apropiado.

Como los servicios basados en RPC confian en `portmap` para hacer todas las conexiones con las peticiones de clientes entrantes, `portmap` debe estar disponible antes que cualquiera de esos servicios comience. Si, por alguna razón, el servicio `portmap` inesperadamente se quita, reinicie `portmap` y cualquier servicio que estuviera ejecutándose entonces.

El servicio `portmap`puede ser usado con los ficheros de accesos de máquinas (`/etc/hosts.allow` y `/etc/hosts.deny`) para controlar a qué sistemas remotos les son permitidos usar servicios basados en RPC en su máquina. Vea el Capítulo 8 para más información. Las reglas de control de acceso para `portmap` afectarán a todos los servicios basados en RPC. Alternativamente, puede especificar a cada uno de los demonios RPC NFS para que sean afectados por una regla de control específica. Las páginas man de `rpc.mountd` y `rpc.statd` contienen información relativa a la sintaxis precisa de estas reglas.

17.1.1.1. Estado de `portmap`

Como `portmap` proporciona la coordinación entre servicios RPC y los números de puertos usados para comunicarlos, es útil plasmar una imagen de los servicios RPC actuales que están usando `portmap` cuando estamos resolviendo algún problema. El comando `rpcinfo` muestra cada servicio basado en RPC con su número de puerto, número de programa RPC, versión y tipo de protocolo (TCP o UDP).

Para asegurarse que los servicios NFS basados en RPC están activos para `portmap`, `rpcinfo -p` puede ser útil:

```
program vers proto   port
 100000    2   tcp    111  portmapper
 100000    2   udp    111  portmapper
 100024    1   udp   1024  status
```

```
100024    1   tcp   1024  status
100011    1   udp    819  rquotad
100011    2   udp    819  rquotad
100005    1   udp   1027  mountd
100005    1   tcp   1106  mountd
100005    2   udp   1027  mountd
100005    2   tcp   1106  mountd
100005    3   udp   1027  mountd
100005    3   tcp   1106  mountd
100003    2   udp   2049  nfs
100003    3   udp   2049  nfs
100021    1   udp   1028  nlockmgr
100021    3   udp   1028  nlockmgr
100021    4   udp   1028  nlockmgr
```

La opción `-p` prueba el portmap de la máquina especificada, o en la maquina local por defecto si no se especifica ninguna máquina. Otras opciones están disponibles en la página manual de `rpcinfo`.

De la salida anterior, varios servicios NFS pueden verse ejecutándose. Si uno de los servicios NFS no comienza correctamente, `portmap` puede ser incapaz de corresponder las peticiones RPC con sus respectivos puertos. En muchos casos, reiniciando NFS como root (`service nfs restart`) provocará que estos servicios funcionen correctamente con `portmap` y empiecen a funcionar.

17.2. Ficheros de configuración del servidor NFS

Es sencillo configurar un sistema para compartir ficheros y directorios usando NFS. Cada Sistema de ficheros que se exporta a usuarios remotos vía NFS, así como los derechos de acceso relativos a ellos, es localizado en el fichero `/etc/exports`. Este fichero es leído por el comando `exportfs` que da a `rpc.mountd` y `rpc.nfsd` la información necesaria para permitir el montaje remoto de un sistema de ficheros por una máquina autorizada.

El comando `exportfs` permite exportar o no directorios concretos sin reiniciar los servicios NFS. Cuando se le pasan las opciones apropiadas a `exportfs`, el sistema de ficheros a exportar es incluido en `/var/lib/nfs/xtab`. Como `rpc.mountd` se refiere al fichero `xtab` para decidir privilegios de acceso a un sistema de ficheros, los cambios en la lista de sistemas de ficheros exportados toman efecto inmediatamente.

Hay varias opciones disponibles cuando usamos `exportfs`:

- `-r` — Provoca que todos los directorios listados en `/etc/exports` sean exportados construyendo una nueva lista de exportación en `/etc/lib/nfs/xtab`. Esta opción refresca la lista de exportación con cualquier cambio que hubiéramos realizado en `/etc/exports`.
- `-a` — Provoca que todos los directorios sean exportados o no, dependiendo de qué otras opciones hemos pasado a `exportfs`.
- `-o` *`opciones`* — Permite al usuario especificar directorios a exportar que no estén listados en `/etc/exports`. Estos sistemas de ficheros adicionales compartidos deben ser escritos de la misma forma que son especificados en `/etc/exports`. Esta opción es usada para probar un sistema de ficheros antes de añadirlo permanentemente a la lista de sistemas a exportar.
- `-i` — Le dice a `exportfs` que ignore `/etc/exports`; solo las opciones dadas en la línea de comandos serán usadas para definir los sistemas de ficheros exportados.
- `-u` — Termina de exportar directorios que puedan ser montados por usuarios remotos. El comando `exportfs -ua` suspende la compartición de ficheros NFS mientras que mantiene los demonios activos. Para continuar con la compartición NFS, teclee `exportfs -r`.

- `-v` — Operación descriptiva, donde los sistemas de ficheros exportados o dejados de exportar son mostrados en gran detalle al ejecutarse el comando `exportfs`.

Si no se pasan opciones al comando `exportfs`, mostrará una lista de los sistemas de ficheros actualmente exportados.

Los cambios efectuados a `/etc/exports` pueden ser leídos al recargar el servicio NFS con el comando `service nfs reload`. Esto deja a los demonios NFS ejecutándose mientras reexporta el fichero `/etc/exports`.

17.2.1. `/etc/exports`

El fichero `/etc/exports` es el estándar para controlar que sistemas de ficheros son exportados a que máquinas, así como para especificar opciones particulares que controlen todo. Las líneas en blanco son ignoradas, se pueden comentar líneas con #, y las líneas largas pueden ser divididas con una barra invertida (\). Cada sistema de ficheros exportado debe tener su propia línea. La lista de máquinas autorizadas colocada después de un sistema de ficheros exportado, debe estar separada por un espacio. Las opciones para cada uno de las máquinas deben ser colocadas entre paréntesis directamente detrás del identificador de la máquina, sin ningún espacio de separación entre la máquina y el primer paréntesis.

De esta sencilla manera, `/etc/exports` solo necesita saber el directorio a exportar y las máquinas que pueden usarlo:

```
/un/directorio bob.domain.com
/otro/directorio/exportado 192.168.0.3
```

Después de reexportar `/etc/exports` con el comando `/sbin/service nfs reload`, la máquina `bob.domain.com` será capaz de montar `/un/directorio`, y `192.168.0.3` podrá montar `/otro/directorio/exportado`. Como no hay opciones especificadas en este ejemplo, varias preferencias por defecto toman efecto:

- `ro` — Solo lectura (read-only). Las máquinas que monten este sistema de ficheros no podrán cambiarlo. Para permitirlas que puedan hacer cambios en el sistema de ficheros, debe especificar la opción `rw` (lectura-escritura - read-write).
- `async` — Permite al servidor escribir los datos en el disco cuando lo crea conveniente. Mientras que esto no tiene importancia en un sistema de solo lectura, si una máquina hace cambios en un sistema de ficheros de lectura-escritura y el servidor se cae o se apaga, se pueden perder datos. Especificando la opción `sync`, todas las escrituras en el disco deben hacerse antes de devolver el control al cliente. Esto bajará el rendimiento.
- `wdelay` — Provoca que el servidor NFS retrase el escribir a disco si sospecha que otra petición de escritura es inminente. Esto puede mejorar el rendimiento reduciendo las veces que se debe acceder al disco por comandos de escritura separados. Use `no_wdelay` para desactivar esta opción, la cual solo funciona si está usando la opción `sync`.
- `root_squash` — Hace que cualquier cliente que acceda al sistema de ficheros exportado (como root en la máquina cliente), se convierta en el ID del usuario nobody. Esto reconvierte el poder del usuario root remoto al de usuario local más bajo, previniendo que los usuarios root remotos puedan convertirse en usuarios root en el sistema local. Alternativamente, la opción `no_root_squash` lo desactiva. Para reconvertir a todos los usuarios, incluyendo a root, use la opción `all_squash`. Para especificar los ID de usuario y grupo para usar con usuarios remotos desde una máquina particular, use las opciones `anonuid` y `anongid` respectivamente. De esta manera, puede crear una cuenta de usuario especial para usuarios NFS remotos para compartir y especificar `(anonuid=`*`<uid-value>`*`,anongid=`*`<gid-value>`*`)`, donde *`<uid-value>`* es el número ID de usuario y *`<gid-value>`* es el número ID de grupo.

Para saltarse estas opciones predeterminadas, debe especificar la opción que desea cambiar. Por ejemplo, si no especifica la opción `rw`, entonces se exportará en solo lectura. Cada opción predeterminada debe ser explícitamente sobreescrita con su opción correspondiente. Adicionalmente, hay otra opciones que están disponibles que no afectan a las predeterminadas. Estas incluyen desactivar el navegar por subdirectorios, permitir el acceso a puertos inseguros, y permitir bloquear ficheros inseguros (necesario para algunas implementaciones antiguas de clientes NFS). Vea la página man de `exports` para estas opciones menos usadas.

Para especificar nombres de host, puede usar los siguientes métodos:

- *una sola máquina* — Cuando una máquina en particular es especificada con nombre completo de dominio, nombre de máquina o dirección IP.
- *comodines* — Cuando usamos un carácter `*` o `?` para referirnos a un grupo de nombres completos de dominio o direcciones IP o que coincidan con una cadena particular de letras.

  Sin embargo, sea cuidadoso cuando use comodines con nombres de dominios completos, e intente ser lo más exacto que pueda. Por ejemplo, el uso de `*.domain.com` como comodín, permitirá a ventas.domain.com acceder al sistema de ficheros exportado, pero no a bob.ventas.domain.com. Para permitir ambas posibilidades, así como a sam.corp.domain.com, debería usar `*.domain.com *.*.domain.com`.
- *redes IP* — Permite el acceso a máquinas basadas en sus direcciones IP dentro de una red más grande. Por ejemplo, `192.168.0.0/15` permite al acceso a las primeras 16 direcciones IP, desde la 192.168.0.0 a la 192.168.0.15, accedes al sistema de ficheros, pero no a la 192.168.0.16 y superiores.
- *grupos de redes* — Permite que un nombre de grupo de red NIS, escrita como `@<group-name>`, sea usada. Esto pone al servidor NIS controlando el acceso de este sistema de ficheros, donde los usuarios pueden ser añadidos o borrados de un grupo NIS sin que afecte a `/etc/exports`.

Atención

La manera en que el fichero `/etc/exports` está organizado es muy importante, particularmente lo que concierne a los espacios en blanco. Recuerde separar siempre los sistemas de ficheros exportados de máquina a máquina y de uno a otro con un espacio. Sin embargo, no debería haber otros espacios en el fichero a menos que se usen en líneas comentadas.

Por ejemplo, las siguientes dos líneas significan cosas distintas:

```
/home bob.domain.com(rw)
/home bob.domain.com (rw)
```

La primera línea permite solo a los usuarios de `bob.domain.com` acceder en modo de lectura-escritura al directorio `/home`. La segunda línea permite a los usuarios de `bob.domain.com` montar el directorio de solo lectura (el predeterminado), pero el resto del mundo puede instalarlo como lectura-escritura. Sea cuidadoso donde se use espacios en blanco en `/etc/exports`.

17.3. Ficheros de configuración de clientes NFS

Cualquier compartición NFS puesta a disposición por un servidor puede ser montada usando varios métodos. Desde luego que puede ser montada manualmente usando el comando `mount`, para adquirir el sistema de ficheros exportado como un punto de montaje concreto. Sin embargo, esto requiere que el usuario root teclee el comando `mount` cada vez que el sistema reinicie. Además, el usuario root debe

recordar desmontar el sistema de ficheros cuando apague la máquina. Otros métodos de configurar los montajes NFS incluyen el modificar `/etc/fstab` o usar el servicio `autofs`.

17.3.1. `/etc/fstab`

Colocando una línea adecuadamente formada en el fichero `/etc/fstab` tiene el mismo efecto que el montaje manual del sistema de ficheros exportado. El fichero `/etc/fstab` es leído por el script `/etc/rc.d/init.d/netfs` cuando arranca el sistema. Los sistemas de ficheros montados, incluyendo NFS, son puestos en su sitio.

Un ejemplo de línea `/etc/fstab` para montar un NFS exportado será parecida a:

```
<server-host>:</path/to/shared/directory>
</local/mount/point> nfs <options> 0 0
```

La opción *<server-host>* tiene que ver con el nombre de la máquina, dirección IP o nombre de domain totalmente cualificado del servidor que exporta el sistema de ficheros. *</path/to/shared/directory>* le dice al servidor que exporta para montar. *</local/mount/point>* especifica dónde, en el sistema de ficheros local, monta el directorio exportado. Este punto de montaje debe existir antes en `/etc/fstab` de donde es leído o el montaje fallará. La opción `nfs` especifica el tipo de sistema de ficheros montado.

El área *<options>* especifica como el sistema de ficheros es montado. Por ejemplo, si las opciones `rw,suid` en un montaje en concreto, el sistema de ficheros exportado será montado en modo de lectura-escritura y los ID de usuario y grupo puestos por el servidor serán usados. Aquí no se usan paréntesis. Para más opciones de montaje, vea la Sección 17.3.3.

17.3.2. `autofs`

Una desventaja de usar `/etc/fstab` es que, sin tener en cuenta cuanto use este sistema de ficheros montado, su sistema debe dedicar recursos a guardar este montaje en su sitio. Esto no es un problema con uno o dos montajes, pero cuando su sistema está manteniendo montajes en una docena de sistemas al tiempo, el rendimiento global puede decaer. Una alternativa a `/etc/fstab` es usar la utilidad basada en el kernel `automount`, la cual monta y desmonta sistemas de ficheros NFS automáticamente, salvando recursos.

El script `autofs`, localizado en `/etc/rc.d/init.d`, es usado para controlar a `automount` a través del fichero de configuración primario `/etc/auto.master`. Mientras que `automount` puede ser especificado en la línea de comandos, es más conveniente especificar los puntos de montaje, nombres de máquinas, directorios exportados y opciones en un conjunto de ficheros que teclearlo todo a mano. Ejecutando `autofs` como servicio que empieza y termina en sus niveles de ejecución designados, las configuraciones de montaje de varios ficheros pueden ser implementados automáticamente. Para usar `autofs`, debe tener al paquete RPM `autofs` instalado en su sistema.

Los ficheros de configuración `autofs` están fijados en una relación padre-hijo. Un fichero principal de configuración (`/etc/auto.master`) se refiere a los puntos de montaje de su sistema que están enlazados a un particular *tipo de mapa*, el cual toma la forma de otros ficheros de configuración, programas, mapas NIS y otros métodos de montaje menos comunes. El fichero `auto.master` contiene líneas referidas a cada punto de montaje, organizadas como:

```
<mount-point>    <map-type>
```

La opción *<mount-point>* indica dónde el dispositivo o sistema de ficheros exportado debe montarse en su sistema local. *<map-type>* muestra la manera como el punto de montaje debe ser montado. El método más común de automontaje de exportaciones NFS es usar un fichero como tipo de mapa del punto de montaje particular. el fichero mapa, usualmente llamado `auto.`*<mount-point>*,

donde *<mount-point>* es el punto de montaje designado en `auto.master`, contiene líneas parecidas a:

<directory> *<mount-options>*
<host>:*<exported-file-system>*

<directory> se refiere al directorio dentro del punto de montaje donde el sistema de ficheros exportado debe ser montado. A menudo, como en el comando estándar `mount`, la máquina que exporta el sistema de ficheros y el sistema de ficheros que está siendo exportado, son requeridos en la sección *<host>*:*<exported-filesystem>*. Para especificar las opciones particulares para montar un sistema de ficheros exportado, colóquelas en la sección *<mount-options>*, separadas por comas. Para montajes NFS que usen `autofs`, debería colocar definitivamente `-fstype=nfs` en la sección *<mount-options>*, como mínimo.

Cómo los ficheros de configuración de `autofs` pueden ser usados para una gran variedad de montajes de muchos tipos de dispositivos y sistemas de ficheros, son particularmente útiles para crear montajes NFS. Por ejemplo, algunas organizaciones guardan un directorio `/home` de usuario en un servidor central vía compartición NFS. Entonces, configuran el archivo `auto.master` en cada una de las estaciones de trabajo para que apunten a un fichero `auto.home` que contiene como montar el directorio `/home` via NFS. Esto permite al usuario acceder a sus datos personales y ficheros de configuración en su directorio `/home` conectándose desde cualquier sitio de la red interna. El fichero `auto.master` en esta situación debería parecerse a:

```
/home   /etc/auto.home
```

Esto hace que el punto de montaje `/home` del sistema local sea configurado con el fichero `/etc/auto.home`, que debe ser similar a:

```
*  -fstype=nfs,soft,intr,rsize=8192,wsize=8192,nosuid  server.domain.com:/home/&
```

Esta línea establece que cualquier directorio bajo el directorio local `/home` al que un usuario intente acceder (debido al asterisco), debe resultar en un punto de montaje NFS en el sistema server.domain.com dentro del sistema de ficheros exportado `/home`. Las opciones de montaje especifican que cada directorio montado via NFS `/home` debe usar una particular colección de opciones. Para más información de las opciones de montaje, incluyendo las usadas en este ejemplo, vea la Sección 17.3.3.

17.3.3. Opciones de montaje NFS comunes

Aparte de montar un sistema de ficheros via NFS en una máquina remota, existe un número de diferentes opciones que pueden ser especificadas en tiempo de montaje que pueden ser más fáciles de usar. Estas opciones pueden usarse con el comando manual `mount`, configuraciones `/etc/fstab`, `autofs` y otros métodos de montaje.

Las siguientes opciones son las más populares para montajes NFS:

- `hard` o `soft` — especifican si el programa que usa un fichero vía conexión NFS debe parar y esperar a que el servidor vuelva a estar en línea si la máquina que exporta ese sistema de ficheros no está disponible (`hard`), o bien debe informar de un error (`soft`).

  Si usa la opción `hard`, no podrá parar el proceso que está esperando la comunicación NFS a menos que especifique la opción `intr`.

  Si usa `soft`, puede usar la opción adicional `timeo=`*<value>*, donde *<value>* especifica el número de segundos que deben pasar antes de informar del error.

- `intr` — permite a las peticiones NFS ser interrumpidas si el servidor se cae o no puede ser accedido.

- `nolock` — es requerido a veces cuando conectamos a servidores NFS antiguos. Para requerir el bloqueo, use la opción `lock`.
- `noexec` — no permite la ejecución de binarios en un sistema de ficheros montado. Esto es útil si su sistema Red Hat Linux está montando un sistema de ficheros no-Linux vía NFS que contiene binarios que no ejecutará en su máquina.
- `nosuid` — no permite que los bits set-user-identifier o set-group-identifier tomen efecto.
- `rsize=8192` y `wsize=8192` — pueden acelerar la comunicación NFS tanto para leer (`rsize`) como para escribir (`wsize`), configurando un tamaño de bloque de datos mayor, en bytes, que serán transferidos de una sola vez. Tenga cuidado al cambiar estos valores; algunos kernels antiguos de Linux y tarjetas de red pueden no trabajar bien con grandes tamaños de bloques.
- `nfsvers=2` o `nfsvers=3` — especifica que versión del protocolo NFS usar.

Hay muchas más opciones en la página del manual de `mount`, incluyendo opciones para montar sistemas de ficheros que no sean NFS.

17.4. Asegurar NFS

NFS trabaja muy bien compartiendo sistemas de ficheros enteros con un gran número de máquinas conocidas de una manera muy trasparente. Muchos usuarios que acceden a ficheros sobre un punto de montaje NFS pueden no estar atentos a que el sistema de ficheros que están usando no está en su sistema local. Sin embargo, esta facilidad de uso trae una variedad de potenciales problemas de seguridad.

Los siguientes puntos deben considerarse cuando exportamos un sistema de ficheros NFS en un servidor o lo montamos en un cliente. Haciendo esto se minimizan los riesgos de seguridad NFS y se mejora la protección de sus datos.

17.4.1. Acceso al sistema

NFS controla quien puede montar y exportar sistemas de ficheros basados en la máquina que lo pide, no el usuario que utilizará el sistema de ficheros. Las máquinas tienen que tener los derechos para montar los sistemas de ficheros exportados explícitamente. El control de acceso no es posible para usuarios, aparte de los permisos de ficheros y directorios. En otras palabras, cuando exporta un sistema de ficheros vía NFS a una máquina remota, no solo está confiando en la máquina a la que permite montar el sistema de ficheros, también está permitiendo a cualquier usuario que acceda a esa máquina que use su sistema de ficheros. Los riesgos de hacer esto pueden controlarse, por ejemplo requiriendo el montaje en solo lectura o cambiando a los usuarios a un ID común de usuario y grupo, pero estas soluciones impiden que el montaje sea usado de la manera originalmente prevista.

Adicionalmente, si un atacante gana el control del servidor DSN usado por el sistema que exporta el sistema de ficheros NFS, el sistema asociado con un nombre de máquina concreto o nombre de dominio totalmente cualificado, puede ser dirigido a una máquina sin autorización. En este punto, la máquina desautorizada *es* el sistema que tiene permitido montar la compartición NFS, ya que no hay intercambio de información de nombre de usuario o contraseña para proporcional seguridad adicional al montaje NFS. Los mismos riesgos corre el servidor NIS, si los nombres de red NIS son usados para permitir a ciertas máquinas montar una compartición NFS. Usando direcciones IP en `/etc/exports`, esta clase de ataques son más difíciles.

Los comodines o metacaracteres deben ser usados lo menos posible cuando garantizamos el acceso a una compartición NFS. El uso de los comodines puede permitir el acceso a sistemas que puede no saber que existen y que no deberían montar el sistema de ficheros.

17.4.2. Permisos de ficheros

Una vez que el sistema de ficheros es montado como lectura-escritura por una máquina remota, la protección de cada fichero compartida depende de sus permisos, y del ID de su usuario y grupo propietario. Si dos usuarios que comparten el mismo valor ID montan el mismo sistema de ficheros NFS, serán capaces de modificarse los ficheros entre sí. Además, cualquiera que esté conectado como root en el sistema cliente, puede usar el comando `su` para convertirse en un usuario que tenga acceso a determinados archivos a través de la compartición NFS.

El procedimiento predeterminado cuando exportamos un sistema de ficheros a través de NFS es usar *root squashing* (sobreponerse a root). Esto cambia el ID de usuario de cualquiera que acceda la compartición NFS, aunque sea el root de su máquina local, al valor de la cuenta nobody del servidor. Nunca debe desactivarlo a menos que no le importe que haya múltiples usuarios con acceso de root en su servidor.

Si solo está permitiendo a los usuarios que lean archivos de su compartición NFS, debería considerar usar la opción `all_squash`, la cual hace que todos los usuarios que accedan a su sistema de ficheros exportado tomen la ID del usuario nobody.

17.5. Recursos adicionales

Administrar un servidor NFS puede ser un desafío. Muchas opciones, incluyendo unas pocas no mencionadas en este capítulo, están disponibles para exportar sistemas de ficheros NFS o montarlos como cliente. Consulte estas fuentes de información para más detalles.

17.5.1. Documentación instalada

- `/usr/share/doc/nfs-utilrs-<version-number>` — Cubre la manera que NFS es implementado en Linux, incluyendo varias configuraciones NFS y su impacto en el rendimiento de transferencia de ficheros.
- Las siguientes páginas del manual son muy útiles:
  - `mount` — Contiene un amplio vistazo a las opciones de montaje tanto a configuraciones de servidores como de clientes NFS.
  - `>fstab` — Da detalles para el formato del fichero `/etc/fstab` usado para montar sistemas de ficheros en el arranque del sistema.
  - `nfs` — Proporciona detalles de opciones de montaje y de exportación de sistemas de ficheros específicos NFS.
  - `exports` — Muestra opciones comunes usadas en el fichero `/etc/exports` cuando exportamos sistemas de ficheros NFS.

17.5.2. Libros relacionados

- *Managing NFS and NIS* por Hal Stern, Mike Eisler, y Ricardo Labiaga; O'Reilly & Associates — Es una guía de referencia excelente para las diferentes opciones NFS disponibles de montaje y exportación.
- *NFS Illustrated* por Brent Callaghan; Addison-Wesley Publishing Company — Proporciona comparaciones entre NFS y otros sistemas de ficheros de red y muestra, en detalle, como las comunicaciones NFS funcionan.

Capítulo 18.

Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (*LDAP*) es una conjunto de protocolos abiertos usados para acceder información guardada centralmente a través de una red. Está basado en el estándar *X.500* para compartir directorios, pero es menos complejo e intensivo en recursos. Por esta razón, a veces se habla de LDAP como *X.500 Lite*.

Como X.500, LDAP organiza la información en un modo jerárquico usando directorios. Estos directorios pueden almacenar variedad de información y se pueden incluso usar en un modo similar al Network Information Service (NIS), permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina en la red activa LDAP.

Sin embargo, en la mayoría de los casos, LDAP se usa simplemente como directorio telefónico virtual, permitiendo a los usuarios acceder fácilmente a información de contacto para otros usuarios. Pero LDAP va más lejos que un directorio telefónico tradicional, ya que es capaz de propagar sus directorios a otros servidores LDAP por todo el mundo, proporcionando acceso global a la información. Sin embargo, en este momento LDAP se usa más dentro de organizaciones individuales, como universidades, departamentos del gobierno y compañías privadas.

LDAP es un sistema cliente-servidor. El servidor puede usar variedad de bases de datos para guardar un directorio, cada uno optimizado para operaciones de lectura rápidas y abundantes. Cuado una aplicación de cliente LDAP se conecta a un servidor LDAP puede, o bien pedir un directorio, o transferir información a él. En el transcurso de una consulta, el servidor, o bien la contesta, o, si no puede contestar localmente, puede dirigir la consulta a un servidor LDAP de un nivel más alto que tenga la respuesta. Si la aplicación de cliente está intentando transferir información a un directorio LDAP, el servidor verifica que el usuario tiene permiso para efectuar el cambio y después añade o actualiza la información.

Este capítulo se hace referencia a la configuración y uso de OpenLDAP 2.1, una implementación open-source del protocolo LDAPv2 y LDAPv3.

18.1. Razones por las que usar LDAP

La mayor ventaja de LDAP es que información para toda una organización se puede consolidar dentro de repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, puede usar LDAP como directorio central accesible desde cualquier parte de la red. Y dado que LDAP soporta Secure Sockets Layer (SSL) y Transport Layer Security (TLS), los datos delicados se pueden proteger de los curiosos.

LDAP soporta también un número de bases de datos back-end en las que se guardan directorios. Esto permite que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que diseminar. También, ya que LDAP tiene un Application Programming Interface (API) bien definido, el número de aplicaciones activadas para LDAP son numerosas y están aumentando en cantidad y calidad.

La parte negativa es que LDAP puede resultar no-trivial a la hora de configurar.

18.1.1. Mejoras en las características de OpenLDAP 2.0

OpenLDAP 2.0 incluye un número de características importantes.

- *Soporte LDAPv3* — OpenLDAP 2.1 soporta Simple Authentication and Security Layer (SASL), Transport Layer Security (TLS), y Secure Sockets Layer (SSL), entre otras mejoras. Muchos de los cambios en el protocolo desde LDAPv2 han sido diseñados para hacer LDAP más seguro.

- *Soporte IPv6* — OpenLDAP soporta la versión 6 del protocolo de Internet de próxima generación.
- *LDAP sobre IPC* — OpenLDAP se puede comunicar dentro de un sistema usando comunicación interproceso (IPC). Esto mejora la seguridad al obviar la necesidad de comunicarse a través de una red.

18.2. Demonios y utilidades OpenLDAP

El paquete de librerías y herramientas OpenLDAP está dentro de los paquetes siguientes:

- `openldap` — Contiene las librerías necesarias para ejecutar las aplicaciones de servidor y cliente openldap.
- `openldap-clients` — Contiene herramientas de línea de comandos para visualizar y modificar directorios en un servidor LDAP.
- `openldap-server` — Contiene los servidores y otras utilidades necesarias para configurar y ejecutar un servidor LDAP.

Hay dos servidores contenidos en el paquete `openldap-servers`: el *Demonio independiente LDAP* (`/usr/sbin/slapd`>) y el *Demonio independiente LDAP con propagación de actualización* (`/usr/sbin/slurpd`).‘

El demonio `slapd` es el servidor real de LDAP mientras que el demonio `slurpd` se usa para sincronizar cambios de un servidor LDAP a otros servidores LDAP en la red. El demonio `slurpd` únicamente es necesario cuando se trata de varios servidores LDAP.

Para llevar a cabo tareas administrativas, el paquete `openldap-server` instala las utilidades siguientes en `/usr/sbin`:

- `slapadd` — Añade entradas de un fichero LDIF a un directorio LDAP. Por ejemplo, `/usr/sbin/slapadd -l` *`ldif-input`* leerá en el fichero LDIF, *`ldif-input`*, Que contiene las nuevas entradas.
- `slapcat` — Extrae entradas de un directorio LDAP y las guarda en un fichero LDIF. Por ejemplo, el comando `/usr/sbin/slapcat -l` *`ldif-output`* tendrá como resultado un fichero LDIF llamado *`ldif-output`* que contendrá las entradas del directorio LDAP.
- `slapindex` — Vuelve a poner en un índice el directorio `slapd` basado en el contenido actual.
- `slappasswd` — Genera un valor de contraseña de usuario cifrada para usar con `ldapmodify` o el valor `rootpw` en el fichero de configuración slapd `/etc/openldap/slapd.conf`. Ejecute `/usr/sbin/slappasswd`para crear la contraseña.

Advertencia

Asegúrese de detener `slapd` ejecutando `/usr/sbin/service slapd stop` antes de usar `slapadd`, `slapcat` o `slapindex`. De otro modo se pondrá en riesgo la consistencia del directorio LDAP.

Para más información sobre cómo utilizar cada una de estas utilidades, consulte las páginas del manual.

El paquete `openldap-clients` instala herramientas utilizadas para añadir, modificar y borrar entradas en un directorio LDAP dentro de `/usr/bin/`. Estas herramientas incluye lo siguiente:

- `ldapmodify` — Modifica entradas en un directorio LDAP, aceptando la entrada por medio de un fichero o entrada estándar.
- `ldapadd` — Añade entradas a su directorio al aceptar la entrada por medio de un fichero o entrada estándar; `ldapadd` es en realidad un link duro a `ldapmodify -a`.
- `ldapsearch` — Busca entradas en el directorio LDAP usando un indicador de comandos shell.
- `ldapdelete` — Borra entradas de un directorio LDAP al aceptar la entrada por medio de la entrada del usuario en la terminal o por medio de un fichero.

A excepción de `ldapsearch`, cada una de estas utilidades se usa más fácilmente haciendo referencia a un fichero que contiene los cambios que se deben llevar a cabo, que escribiendo un comando para cada entrada que se desea cambiar en un directorio LDAP. El formato de dicho fichero está esquematizado en las páginas del manual sobre cada aplicación.

Red Hat Linux incluye una aplicación gráfica llamada **GQ** que soporta las funciones de crear y modificar entradas de directorio. Esta aplicación no es parte de el conjunto de herramientas OpenLDAP, sino que está dentro de `gq` rpm. Consulte la Sección 18.2.3 para más información sobre aplicaciones de cliente LDAP.

18.2.1. NSS, PAM y LDAP

Además de los paquetes OpenLDAP, Red Hat Linux incluye un paquete llamado `nss_ldap` que mejora la capacidad de LDAP de integrar LDAP dentro de entornos tanto de Linux como de UNIX.

El paquete `nss_ldap` proporciona los módulos siguientes:

- `/lib/libnss_ldap-2.2.90.so`
- `/usr/lib/libnss_ldap.so`
- `/lib/security/pam_ldap.so`

Los módulos `/lib/libnss_ldap-2.2.90.so` y `/usr/lib/libnss_ldap.so` permiten que las aplicaciones busquen al usuario, grupo, host y otra información utilizando un directorio LDAP por medio de la interfaz *Nameservice Switch* (NSS). NSS se puede usar en lugar de o junto con la información de *Network Information Service* (NIS) para autenticación.

El módulo `pam_ldap` permite que las aplicaciones PAM puedan autentificar usuarios utilizando información guardada en un directorio LDAP. Las aplicaciones PAM incluyen terminales, servidores de correo POP e IMAP, y Samba. Al desarrollar un servidor LDAP en su red, todas estas situaciones de login pueden autentificarse contra una combinación de ID y contraseña de usuario, simplificando así en gran medida la administración.

18.2.2. El Servidor HTTP de Apache, PHP4 y LDAP

Red Hat Linux incluye también paquetes que contienen módulos LDAP para el lenguaje escrito por el servidor Servidor HTTP de Apache y PHP.

El paquete `auth_ldap` contiene el módulo LDAP para Servidor HTTP de Apache llamado `mod_auth_ldap.so`. Esta módulo permite al Servidor HTTP de Apache autentificar usuarios usando información guardada en un directorio LDAP.

El paquete `php-ldap` añade soporte de LDAP al lenguaje escrito PHP4 HTML-embedded por medio del módulo `/usr/lib/php4/ldap.so`. Este módulo permite que scripts PHP4 accedan a información guardada en un directorio LDAP.

18.2.3. Aplicaciones de cliente LDAP

Fuera de las herramientas de la línea de comandos en el equipo OpenLDAP, la aplicación de cliente LDAP primaria incluida con Red Hat Linux 8.0 es **GQ**. **GQ** es un cliente LDAP gráfico basado en GTK que soporta el cifrado a través de TLS y permite crear y modificar directorios.

Hay otros clientes LDAP gráficos disponibles que soportan la función de crear y modificar directorios, pero que no funcionan con Red Hat Linux 8.0. Una de estas aplicaciones es **LDAP Browser/Editor** — Una herramienta basada en Java que se encuentra disponible en http://www.iit.edu/~gawojar/ldap.

La mayoría de otros clientes LDAP acceden a directorios as read-only, usándolos como referencia, pero sin alterar información de toda la organización. Algunos ejemplos de dichas aplicaciones son browsers de red basados en Mozilla, Sendmail **Balsa**, **Pine**, **Evolution**, **Gnome Meeting**.

18.3. Terminología LDAP

Una *entrada* es una unidad en un directorio LDAP. Cada entrada se identifica por su único Distinguished Name (DN).

Cada entrada tiene *atributos*, que son piezas de información Directamente asociada con la entrada. Por ejemplo, una organización podría ser una entrada LDAP. Atributos asociados a la organización podrían ser el número de fax, la dirección, etc. En un directorio LDAP las entradas pueden ser también personas. Atributos comunes de las personas como el número de teléfono y la dirección de e-mail.

Algunos atributos son obligatorios mientras que otros son opcionales. Una definición *objectclass* determina qué atributos se requieren y cuáles no para cada entrada. Las definiciones de objectclass se encuentran en varios ficheros dentro del directorio `/etc/openldap/schema/`.

El *Formato de intercambio de datos LDAP* (LDIF) es un formato de texto ASCII para entradas LDAP. Los ficheros que importan y exportan datos de y a servidores LDAP deben estar en formato LDIF. Una entrada LDIF es parecida al ejemplo siguiente:

```
[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
```

Una entrada puede contener tantas líneas emparejadas `<attrtype>: <attrvalue>` como sean necesarios. Una línea en blanco indica el final de una entrada.

Advertencia

Las parejas `<attrtype>` y `<attrvalue>` *deben* ser definidas en un fichero esquema para usar esta información.

Cualquier valor comprendido dentro de < y > es una variable y puede ser configurado cuando se cree una nueva entrada LDAP, excepto para `<id>`. El `<id>` es un número determinado por la aplicación que usa para editar la entrada.

Nota

No debería tener nunca la necesidad de editar una entrada LDIF a mano. En lugar de esto use Una aplicación de cliente LDAP, como las que aparecen en Sección 18.2.

18.4. Ficheros de configuración OpenLDAP

Los ficheros de configuración OpenLDAP se instalan dentro del directorio `/etc/openldap/`. A continuación aparece una lista breve marcando los directorios y ficheros más importantes:

- `/etc/openldap/schema/` directorio — Este subdirectorio contiene el esquema usado por el demonio `slapd`. Consulte Sección 18.4.2 para más información sobre este directorio.
- `/etc/openldap/ldap.conf` — Este fichero es el fichero configuración para todas las aplicaciones *client* que usan las librerías OpenLDAP. Éstas incluyen, pero no se limitan a, Sendmail, **Pine**, **Balsa**, **Evolution** y **Gnome Meeting**.
- `/etc/openldap/slapd.conf` — Éste es el fichero configuración para el demonio `slapd`. Consulte Sección 18.4.1 para más información sobre este fichero.

Note

Si se instala el paquete `nss_ldap`, creará un fichero llamado `/etc/ldap.conf`. Este fichero es usado por los módulos PAM y NSS proporcionados por el paquete `nss_ldap`. Consulte Sección 18.7 para más información sobre este fichero de configuración.

18.4.1. `slapd.conf`

Para usar el servidor LDAP `slapd`, tendrá que modificar su fichero de configuración, `/etc/openldap/slapd.conf`. Debe editar este fichero para hacerlo específico a su dominio y a su servidor.

La línea `suffix` da nombre al dominio para el que el servidor LDAP proporcionará información. La línea `suffix` debería cambiarse desde:

```
suffix          "dc=your-domain, dc=com"
```

de modo que refleje su nombre de dominio. Por ejemplo:

```
suffix          "dc=subgenius, dc=com"
```

La entrada `rootdn` es el *Distinguished Name* (*DN*) para un usuario que no está restringido por el control de acceso o los parámetros de límite administrativos fijados para operaciones en el directorio LDAP. Se puede pensar en el usuario `rootdn` como el usuario raíz para el directorio LDAP. La línea `rootdn` debe cambiar de:

```
rootdn          "cn=root, dc=your-domain, dc=com"
```

a algo parecido a :

```
rootdn          "cn=root, dc=subgenius, dc=com"
```

Cambie la línea `rootpw` a algo parecido al ejemplo que aparece a continuación:

```
rootpw          {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

En el ejemplo `rootpw`, está usando una contraseña raíz cifrada, lo que es mejor que dejar una contraseña raíz de solo texto en el fichero `slapd.conf`. Para hacer esta cadena cifrada, escriba el comando siguiente:

```
slappasswd
```

Se le pedirá que escriba y rescriba una contraseña. El programa imprime la contraseña cifrada resultante a la terminal.

Advertencia

Las contraseñas LDAP, incluyendo la directriz `rootpw` especificada en `/etc/openldap/slapd.conf`, se envían a través de la red como solo texto a menos que active el cifrado TLS.

Para mayor seguridad, la directriz `rootpw` debería usarse únicamente si la configuración inicial y la población del directorio LDAP ocurre a través de la red. Después de que le tarea se haya completado, es mejor anunciar la directriz `rootpw` precediéndola con con un signo como éste(#).

Tip

Si está usando la herramienta de la línea de comandos `slapadd` localmente para poblar el directorio LDAP, no es necesario usar la directriz `rootpw`.

18.4.2. El directorio `/etc/openldap/schema/`

El directorio `/etc/openldap/schema/` contiene definiciones LDAP, que antes se encontraban en los ficheros `slapd.at.conf` y `slapd.oc.conf`. Todos las *definiciones de sintaxis de atributo* y *definiciones objectclass* se encuentran ahora en los diferentes ficheros de esquema. A éstos se hace referencia en `/etc/openldap/slapd.conf` usando líneas `include`, como se muestra en el siguiente ejemplo:

```
include  /etc/openldap/schema/core.schema
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/rfc822-MailMember.schema
include  /etc/openldap/schema/autofs.schema
include  /etc/openldap/schema/kerberosobject.schema
```

Atención

No debería modificar ningún artículo del esquema definido en los archivos de esquema instalados por **OpenLDAP**.

```
include          /etc/openldap/schema/local.schema
```

A continuación, Defina los tipos de atributos y las clases de objetos en el archivo `local.schema`. Muchas organizaciones utilizan tipos de atributos y clases de objetos de los ficheros de esquema

instalados por defecto y los modifica para usarlos en el fichero `local.schema`. Esto puede ayudarle a aprender la sintaxis del esquema mientras que se corresponde con las necesidades de su organización.

Ampliar esquemas para cumplir determinados criterios especializados tiene bastante que ver y Va más allá del propósito de este capítulo. Consulte http://www.openldap.org/doc/admin/schema.html para más información sobre cómo escribir nuevos ficheros esquema.

18.5. Vista preliminar de la configuración de OpenLDAP

Esta sección explica rápidamente la instalación y la configruación del directorio OpenLDAP. Para más información, consulte las URLs siguientes:

- http://www.openldap.org/doc/admin/quickstart.html — El manual *Quick-Start Guide* en la página web de OpenLDAP.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — El *LDAP Linux HOWTO* del Proyecto de documentación de Linux, Reflejado en la página web de Red Hat's.

Los pasos básicos para crear un servidor LDAP son los siguientes:

1. Instale los RPMs `openldap`, `openldap-servers` y `openldap-clients`.
2. Edite el fichero `/etc/openldap/slapd.conf` para hace referencia al dominio y servidor LDAP. Consulte Sección 18.4.1 para más información sobre cómo editar este fichero.
3. Inicie `slapd` con el comando:
   `/sbin/service/ldap start`

   Después de que haya configurado correctamente LDAP, puede usar `chkconfig`, `ntsysv` o **redhat-config-services** para configurar LDAP de modo que se inicie al arrancar. Para más información sobre cómo configurar servicios, consulte el capítulo titulado *Controlar el acceso a servicios* en la *Official Red Hat Linux Customization Guide*.
4. Añada entradas a su directorio LDAP con `ldapadd`.
5. Use `ldapsearch` para ver si `slapd` accede a la información correctamente.
6. Llegados a este punto, su directorio LDAP debería funcionar correctamente y entonces puede configurar aplicaciones habilitadas para LDAP para que usen el directorio LDAP.

18.6. Actualización de OpenLDAP a la versión 2.0

En la versión OpenLDAP 2.0, el formato de almacenamiento usado por el servidor LDAP `slapd` ha cambiado. Si está actualizando LDAP 7.0 o anterior, necesitará extraer los directorios LDAP para un fichero LDIF usando el siguiente comando:

```
ldbmcat -n > <ldif_file>
```

En el comando de arriba, cambie *<ldif_file>* al nombre del fichero de la salida. A continuación escriba el siguiente comando para importar este fichero en OpenLDAP 2.0:

```
slapadd -l <ldif_file>
```

18.7. Configurar su sistema para la autenticación mediante OpenLDAP

Este apartado ofrece una supervisión de cómo configurar un sistema Red Hat Linux para autenticarse con el uso de OpenLDAP. A menos que usted sea un experto de OpenLDAP, necesitará más documentación que la proporcionada. Para obtenerla remítase a la Sección 18.8

18.7.1. Instalación de los paquetes LDAP necesarios

En primer lugar asegúrese de que los paquetes apropiados son instalados tanto en el servidor LDAP como en las máquinas cliente LDAP. El servidor LDAP necesita el paquete `openldap-server`.

Las máquinas cliente LDAP necesitan de la instalación de los siguientes paquetes: `openldap`, `openldap-clients` y `nss_ldap`.

18.7.2. Modificar los ficheros de configuración

18.7.2.1. En el servidor,modificar `slapd.conf`

Modifique el fichero `/etc/openldap/slapd.conf` para asegurarse de que se adapta a las necesidades de su organización. Remítase a la Sección 18.4.1 para ulterior información sobre modificar `slapd.conf`.

18.7.2.2. En clientes, modifique `/etc/ldap.conf` y `/etc/openldap/ldap.conf`

Todos las máquinas de los clientes, ambas `/etc/ldap.conf` y `/etc/openldap/ldap.conf` necesitan el servidor más adecuado y buscan la información de base para su organización.

La forma más sencilla de realizarlo es ejecutar la aplicación **authconfig** y seleccionar **Usar LDAP** en la pantalla **Configuración de la información del usuario**.

Modifique el fichero `/etc/ldap.conf` en el servidor LDAP y en los clientes.

18.7.2.3. En clientes, modifique `/etc/nsswitch.conf`

En todas las máquinas cliente, `/etc/nsswitch.conf` debe modificarse para usar LDAP.

El modo más sencillo de realizarlo es ejecutar la aplicación **authconfig** y seleccionar **Usar LDAP** en la pantalla **Configuración de la información de usuario**.

Al modificar `/etc/nsswitch.conf` a mano, `ldap` al campo apropiado.

Por ejemplo:

```
passwd: files ldap
shadow: files ldap
group: files ldap
```

18.7.2.4. PAM y LDAP

Para tener las aplicaciones estándar PAM use LDAP para autenticación, ejecute `authconfig` y seleccione **Usar LDAP**. Para obterner más información sobre cómo configurar PAM consulte el Capítulo 7 y/o las páginas de manual de PAM.

18.7.3. Migrar el viejo método de autenticación al formato LDAP

El directorio `/usr/share/openldap/migration` contiene un conjunto de scripts de shell y Perl para cambiar métodos de autenticación al formato LDAP.

Nota

Debe tener Perl instalado en su sistema para usar estos scripts.

En primer lugar deberá modificar el fichero `migrate_common.ph` de manera que refleje su dominio. El dominio DNS por defecto debería cambiarse de su valor por defecto a algo parecido a:

```
$DEFAULT_MAIL_DOMAIN =
"su_compañía.com";
```

También la base por defecto debería cambiarse a algo como:

```
$DEFAULT_BASE =
"dc=su_compañía,dc=com";
```

La tarea de migrar una base de datos de usuario a un formato que pueda leer LDAP le corresponde a un grupo de scripts de migración instalado con el paquete `nss_ldap`. Al usar Tabla 18-1, se decide qué script ejecutar para migrar su base de datos de usuario.

Nombre actual del servicio	¿LDAP está activado?	Utilice este script:
`/etc` flat files	sí	`migrate_all_online.sh`
`/etc` flat files	no	`migrate_all_offline.sh`
NetInfo	sí	`migrate_all_netinfo_online.sh`
NetInfo	no	`migrate_all_netinfo_offline.sh`
NIS (YP)	sí	`migrate_all_nis_online.sh`
NIS (YP)	no	`migrate_all_nis_offline.sh`

Tabla 18-1. Scripts de migración a LDAP

Ejecute el script adecuado basándose en su nombre de servicio actual.

Los ficheros `README` y `migration-tools.txt` en el directorio `/usr/share/openldap/migration` proporcionan más detalles sobre cómo migrar información.

18.8. Recursos adicionales

En la web puede encontrar más información útil referente a LDAP. Use estos recursos, en especial visite el sitio web OpenLDAP y el LDAP HOWTO, antes de iniciar e introducir LDAP en su sistema.

18.8.1. Documentación instalada

- La página de manual `ldap` es un buen lugar donde empezar a documentarse sobre LDAP. Existen también páginas de manual para los demonios y las utilidades LDAP.
- `/usr/share/docs/openldap-`*`versionnumber`* — contiene un documento general `README` e información variada.

18.8.2. Sitios Web útiles

- http://www.openldap.org — Portal del proyecto OpenLDAP. Esta página web contiene gran cantidad de información sobre cómo configurar LDAP.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Un LDAP HOWTO viejo, pero que aún es relevante.
- http://www.padl.com — Desarrolladores de `nss_ldap` and `pam_ldap`, entre otras herramientas útiles de LDAP.
- http://www.innosoft.com/ldapworld — Contiene información referente a las versiones LDAP RFCs y LDAP versión 3.
- http://www.kingsmountain.com/ldapRoadmap.shtml — El "mapa de carreteras" de LDAP de Jeff Hodges contiene enlaces a diversas FAQs útiles y emite noticias referentes al protocolo LDAP.
- http://www.rudedog.org/auth_ldap — Sitio del módulo de autenticación `auth_ldap` para el Servidor HTTP de Apache.
- http://www.webtechniques.com/archives/2000/05/wilcox — Un vistazo útil para gestionar grupos en LDAP.
- http://www.ldapman.org/articles — Artículos que ofrecen una buena introducción a LDAP, incluyendo métodos para diseñar un árbol de directorio y estructuras de directorio personalizadas.

18.8.3. Libros relacionados

- *Implementing LDAP* de Mark Wilcox; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* de Tim Howes et al.; Macmillan Technical Publishing

Apéndices

Apéndice A.

Parámetros generales y módulos

Este apéndice ilustra *algunos* de los posibles parámetros disponibles para algunos controladores de dispositivos de hardware comunes[1] En la mayoría de casos, estos parámetros adicionales son innecesarios, ya que el kernel es capaz de usar el dispositivo sin ellos. Utilice las configuraciones proporcionadas en este apéndice si tiene problemas para hacer que Red Hat Linux utilice un dispositivo determinado o si necesita sobreescribir los parámetros predeterminados del sistema para el dispositivo.

Durante la instalación de Red Hat Linux, se establecen determinados límites al sistema de ficheros y a algunos de los controladores de dispositivos soportados por el kernel. Sin embargo, después de la instalación se proporciona soporte a todos los sistemas de ficheros disponibles bajo Linux. En el momento de la instalación, el kernel modular proporciona soporte a dispositivos (E)IDE (incluyendo unidades CDROMs ATAPI), adaptadores SCSI y tarjetas de red.

Nota

Dado que Red Hat Linux soporta la instalación en diversas plataformas de hardware, algunos controladores (incluyendo aquéllos para adaptadores SCSI, tarjetas de red y algunos CDROMs) no son compilados en el interior del kernel de Linux utilizado durante la fase de instalación, pero están disponibles como módulos y son cargados cuando hagan falta en el proceso de instalación. Si fuese necesario, tiene la posibilidad de especificar las opciones para estos módulos en el momento en que se carguen desde el disco de controladores.

Para especificar los parámetros de los módulos cuando se carga un controlador, teclee **`linux expert`** en el indicador de comandos `boot:` que aparecerá al iniciar su sistema e inserte el disco de controladores cuando se lo indique el programa de instalación. Tras haber leído el disco de controladores, el programa de instalación le pedirá que seleccione el tipo de dispositivo que está configurando. A continuación, el programa de instalación mostrará una pantalla donde puede escribir los parámetros correctos basados en el tipo determinado de dispositivo que está configurando.

Una vez completada la instalación podría querer volver a compilar el kernel para incluir el soporte a su configuración hardware específica. Observe que en la mayoría de los casos, no es necesario un kernel personalizado. Consulte el *Manual oficial de personalización de Red Hat Linux* para obtener información sobre cómo construir un kernel personalizado.

A.1. Especificación de parámetros de los módulos

Si quiere proporcionar parámetros para cargar un módulo, podrá especificarlos usando uno o dos métodos diferentes:

- Especifique un conjunto completo de parámetros en una frase. Por ejemplo, el parámetro `cdu31=0x340,0` podría ser utilizado con un CDU 31 de Sony en el puerto 340 sin IRQ.
- Especifique los parámetros individualmente. Este método se usa cuando no son necesarios uno o más parámetros en el primer grupo. Por ejemplo, `cdu31_port=0x340 cdu31a_irq=0` puede ser usado como el parámetro para el mismo CD-ROM usado como ejemplo para el primer método. Se

1. Un *controlador/driver de dispositivos* es un tipo de software que ayuda a su sistema usar un determinado dispositivo hardware. Sin el controlador de dispositivos, el kernel no sabría cómo acceder a este dispositivo correctamente.

utiliza un *OR* las tablas de CD-ROM, SCSI y Ethernet en este apéndice para mostrar el punto en el que el primer método de parámetros se detiene y el segundo método empieza.

Nota

Utilice solo un método y no ambos cuando cargue un módulo con parámetros particulares.

Advertencia

Cuando un parámetro tenga comas, asegúrese de que *no* deja un espacio tras una coma.

A.2. Parámetros del módulo de CD-ROM

Nota

No todas las unidades de CD-ROM listadas son soportadas. Verifique para más seguridad la lista de las compatibilidades de hardware en el sitio Web de Red Hat en la dirección web http://hardware.redhat.com para asegurarse de que se soporta su unidad de CD-ROM.

Aunque los parámetros sean especificados tras cargar el disco de controladores y especificar el dispositivo, uno de los parámetros usados más comunmente (`hd`*`X`*`=cdrom`) *puede* ser introducido en el indicador de comandos de arranque (`boot:`) durante la instalación. Esta excepción a la regla es permitida porque trata con el soporte para los CD-ROMs IDE/ATAPI, que forman parte del kernel.

En las tablas que se detallan a continuación, muchos módulos se enumeran sin parámetros porque, o son capaces de efectuar automáticamente un control o bien le piden que modifique manualmente los parámetros en el código fuente del módulo y que después recompile.

Hardware	Módulo	Parámetros
Unidades ATAPI/IDE CD-ROM Drives		hd*X*=cdrom
Aztech CD268-01A, Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CR520, CyCDROM CR540 (no-IDE)	`aztcd.o`	aztcd=*`io_port`*
Sony CDU-31A CD-ROM	`cdu31a.o`	cdu31a=*`io_port`*,*`IRQ`* *OR* cdu31a_port=*`base_addr`* cdu31a_irq=*`irq`*
Unidad de CDROM Philips/LMS CDROM 206 con tarjeta de adaptador host cm260	`cm206.o`	cm206=*`io_port`*,*`IRQ`*

Hardware	Módulo	Parámetros
Goldstar R420 CD-ROM	`gscd.o`	gscd=*`io_port`*
Interfaz CD-ROM de las tarjetas de sonido ISP16, MAD16, o Mozart (OPTi 82C928 y OPTi 82C929) con lector Sanyo/Panasonic, Sony o Mitsumi	`isp16.o`	isp16=*`io_port`*,*`IRQ`*,*`dma`*, *`drive_type`* *OR* isp16_cdrom_base=*`io_port`* isp16_cdrom_irq=*`IRQ`* isp16_cdrom_dma=*`dma`* isp16_cdrom_type=*`drive_type`*
Mitsumi CD-ROM,estándar	`mcd.o`	mcd=*`io_port`*,*`IRQ`*
Mitsumi CD-ROM, experimental	`mcdx.o`	mcdx=*`io_port_1`*,*`IRQ_1`*, *`io_port_n`*,*`IRQ_n`*
Unidad de almacenamiento óptica 8000 AT "Dolphin", Lasermate CR328A	`optcd.o`	
CD-ROM IDE de puerto paralelo	`pcd.o`	
Tarjeta sonido compatible SB Pro 16	`sbpcd.o`	sbpcd=*`io_port`*
Sanyo CDR-H94A	`sjcd.o`	sjcd=*`io_port`* *OR* sjcd_base=*`io_port`*
Sony CDU-535 & 531 (algunas unidades Procomm)	`sonycd535.o`	sonycd535=*`io_port`*

Tabla A-1. Parámetros hardware

A continuación le mostramos algunos ejemplos de la utilización de estos módulos:

Configuración	Ejemplo
CD-ROM ATAPI, puenteado como maestro en el segundo canal IDE	hdc=cdrom
CD-ROM Mitsumi no IDE en el puerto 340, IRQ 11	mcd=0x340,11
Tres lectores de CD-ROM Mitsumi no IDE que utilizan el controlador experimental, en los puertos de E/S 300, 304 y 320 con IRQs 5, 10 y 11	mcdx=0x300,5,0x304,10,0x320,11
Sony CDU 31 o 33 en el puerto 340, sin IRQ	cdu31=0x340,0 *OR* cdu31_port=0x340 cdu31a_irq=0
CD-ROM Aztech en el puerto 220	aztcd=0x220
CD-ROM de tipo Panasonic en una interfaz SoundBlaster en el puerto 230	sbpcd=0x230,1
Phillips/LMS cm206 y cm260 en ES 340 y con IRQ 11	cm206=0x340,11
Goldstar R420 en ES 300	gscd=0x300

Configuración	Ejemplo
Unidad Mitsumi en una tarjeta de sonido MAD16 en la dirección ES 330 y con IRQ 1, probando DMA	isp16=0x330,11,0,Mitsumi
Sony CDU 531 en la dirección ES 320	sonycd535=0x320

Tabla A-2. Ejemplos de configuración de parámetros de hardware

Nota

La mayoría de tarjetas Sound Blaster nuevas tienen una interfaz IDE. Para estas tarjetas, no es necesario utilizar los parámetros `sbpcd`, utilice solo los parámetros `hdX`.

A.3. parámetros SCSI

Hardware	Módulo	Parámetros
Adaptec 28xx, R9xx, 39xx	`aic7xxx.o`	
Controlador de almacenamiento de 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Driver AM53/79C974 (PC-SCSI) Driver	`AM53C974.o`	
Casi todas las tarjetas Buslogic (actualmente Mylex) con número "BT"	`BusLogic.o`	BusLogic_Options=*`option`*,*`option`*`,...`
Controlador RAID Mylex DAC960	`DAC960.o`	
SCSI basado en MCR53c406a	`NCR53c406a.o`	
Initio INI- A100U2W	`a100u2w.o`	a100u2w=*`io`*,*`IRQ`*,*`scsi_id`*
Adaptec AACRAID	`aacraid.o`	
Tarjetas SCSI de Advansys	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*`io`*,*`IRQ`*,*`scsi_id`*
Adaptec AHA 154x y basadas en 631x	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	

Hardware	Módulo	Parámetros
Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x , AIC-789x, AIC-3860	`aic7xxx.o`	aic7xxx=*`string`*
Controlador SCSI ACARD ATP870U PCI	`atp870u.o`	
Controlador Compaq Smart Array 5300	`cciss.o`	
Controlador RAID Compaq Smart/2	`cpqarray.o`	
Controlador Compaq FibreChannel	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
Data Technology Corp DTC3180/3280	`dtc.o`	
Adaptadores host SCSI DTP (EATA/DMA) PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	eata=*`port0`*,*`port1`*,*`port2`*,*`...`* *`options`* *OR* eata io_port=*`port0`*,*`port1`*,*`port2`*,*`...`* option=*`value`*

Hardware	Módulo	Parámetros
Adaptadores hosts SCSI DTP Adapters PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
DTP EATA-PIO boards	`eata_pio.o`	
Sun Enterprise Network Array (FC-AL)	`fcal.o`	
Future Domain TMC-16*xx* SCSI	`fdomain.o`	
NCR5380 (controlador genérico)	`g_NCR5380.o`	
Controlador RAID ICP	`gdth.o`	
Controlador de bloques I2O	`i2o_block.o`	
Adaptador SCSI en puerto paralelo IOMEGA MatchMaker	`imm.o`	
Tarjeta SCSI ISA Always IN2000	`in2000.o`	in2000=*`setup_string`*:*`value`* *O* in2000 *`setup_string=value`*
Adaptadores de host SCSI Initio INI-9X00U/UW	`initio.o`	
ServeRAID IBM	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
Controladores SCSI INCR con chipsets 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=*`option1`*:*`value1`*, *`option2`*:*`value2,...`* *OR* ncr53c8xx="*`option1`*:*`value1 option2`*:*`value2...`*"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	
RAID PCI-2220I EIDE	`pci2220i.o`	
Array SparcSTORAGE	`pluto.o`	
Adaptador de host SCSI en puerto paralelo IOMEGA PPA3	`ppa.o`	

Hardware	Módulo	Parámetros
Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
Qlogic 1280	`qla1280.o`	
Qlogic 2*x*00	`qla2x00.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
Tarjetas QLogic ISP1020 Intelligent SCSI IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
Qlogic ISP1020 SCSI SBUS	`qlogicpti.o`	
Future Domain TMC-885, TMC-950 Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	controller_type=2 base_address=*`base_addr`* irq=*`IRQ`*
Tarjetas con el chipset sym53c416	`sym53c416.o`	sym53c416=*`PORTBASE`*,*`[IRQ]`* *OR* sym53c416 io=*`PORTBASE`* irq=*`IRQ`*
Adaptador de host SCSI Trantor T128/T128F/T228	`t128.o`	
Tekram DC-390(T) PCI	`tmscsim.o`	
UltraStor 14F/34F (not 24F)	`u14-34f.o`	
UltraStor 14F, 24F y 34F	`ultrastor.o`	
Series WD7000	`wd7000.o`	

Tabla A-3. Parámetros SCSI

Le mostramos algunos ejemplos sobre la utilización de estos parámetros:

Configuración	Ejemplo
Adaptec AHA1522 en el puerto 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 en el puerto 330	bases=0x330
Future Domain TMC-800 en CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

Tabla A-4. Ejemplos de configuración de parámetros SCSI

A.4. Parámetros Ethernet

Hardware	Módulo	Parámetros
3Com 3c501	`3c501.o`	3c501=*`io_port,IRQ`*
3Com 3c503 y 3c503/16	`3c503.o`	3c503=*`io_port`*,*`IRQ`* *OR* 3c503 io=*`io_port_1`*,*`io_port_n`* irq=*`IRQ_1`*,*`IRQ_n`*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=*`io_port,IRQ`* *OR* 3c505 io=*`io_port_1`*,*`io_port_n`* irq=*`IRQ_1`*,*`IRQ_2`*
3Com EtherLink 16	`3c507.o`	3c507=*`io_port,IRQ`* *OR* 3c507 io=*`io_port`* irq=*`IRQ`*
3Com EtherLink III	`3c509.o`	3c509=*`IRQ`*
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
Tarjetas RealTek que usen los chipsets RTL8129 o RTL8139 de Fast Ethernet	`8139too.o`	
Apricot 82596	`82596.o`	
Ansel Communications Model 3200	`ac3200.o`	ac3200=*`io_port`*,*`IRQ`* *O* ac3200 io=*`io_port_1`*,*`io_port_n`* irq=*`IRQ_1`*,*`IRQ_n`*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Allied Telesis AT1700	`at1700.o`	at1700=*`io_port`*,*`IRQ`* *O* at1700 io=*`io_port`* irq=*`IRQ`*
Crystal Semiconductor CS89[02]0	`cs89x0.o`	

Hardware	Módulo	Parámetros
Tarjetas EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, tarjetas Znyx31[45], y Znyx346 10/100 con chipsets DC21040 (no SROM), DC21041[A], DC21140[A], DC21142, DC21143	`de4x5.o`	de4x5=*`io_port`* *OR* de4x5 io=*`io_port`* de4x5 args='eth*`X[fdx]`* autosense=*`MEDIA_STRING`*'
Adaptador de bolsillo Ethernet D-Link DE-600	`de600.o`	
Adaptador de bolsillo Ethernet D-Link DE-620	`de620.o`	
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca=*`io_port`*,*`IRQ`* *OR* depca io=*`io_port`* irq=*`IRQ`*
Digi Intl. RightSwitch SE-X EISA y PCI	`dgrs.o`	
Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*`io_port`*,*`IRQ`*,*`mem`* *OR* e2100 io=*`io_port`* irq=*`IRQ`* mem=*`mem`*
Intel EtherExpress Pro10	`eepro.o`	eepro=*`io_port`*,*`IRQ`* *OR* eepro io=*`io_port`* irq=*`IRQ`*
Intel i82557/i82558 PCI EtherExpressPro driver	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=*`io_port`*,*`IRQ`* *O* eexpress io=*`io_port`* irq=*`IRQ`*
SMC EtherPower II 9432 PCI (83c170/175 EPIC series)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i=*`io_port`*,*`IRQ`* *OR* eth16i ioaddr=*`io_port`* IRQ=*`IRQ`*

Hardware	Módulo	Parámetros
EtherWORKS 3 (DE203, DE204 y DE205)	`ewrk3.o`	ewrk=*`io_port`*,*`IRQ`* *O* ewrk io=*`io_port`* irq=*`IRQ`*
Packet Engines GNIC-II Gigabit	`hamachi.o`	
HP PCLAN/plus	`hp-plus.o`	hp-plus=*`io_port`*,*`IRQ`* *OR* hp-plus io=*`io_port`* irq=*`IRQ`*
HP LAN Ethernet	`hp.o`	hp=*`io_port`*,*`IRQ`* *OR* hp io=*`io_port`* irq=*`IRQ`*
Adaptador de red 100VG-AnyLan HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=*`io_port`*,*`name`* *O* hp100 hp100_port=*`io_port`* hp100_name=*`name`*
IBM Token Ring 16/4	`ibmtr.o`	ibmtr=*`io_port`*,*`IRQ`*,*`mem`* *OR* ibmtr io=*`io_port`* irq=*`IRQ`* mem=*`mem`*
AT1500, HP J2405A, la mayoría de NE2100/clone	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
NE1000 / NE2000 (no-pci)	`ne.o`	ne=*`io_port`*,*`IRQ`* *O* ne io=*`io_port`* irq=*`IRQ`*
Tarjetas PCI NE2000 RealTEk RTL-8029, Winbond 89C940, Compex RL2000, KTI ET32P2, NetVin, NV5000SC, Via 82C926, SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
Tarjeta NI5210 (chip i82586 Ethernet)	`ni52.o`	ni52=*`io_port`*,*`IRQ`* *OR* ni52 io=*`io_port`* irq=*`IRQ`*
NI6510 Ethernet	`ni65.o`	
AMD PCnet32 y AMD PCnetPCI	`pcnet32.o`	
SysKonnect SK-98*XX* Gigabit	`sk98lin.o`	
Tarjetas ether SMC Ultra y SMC EtherEZ ISA (8K, 83c790)	`smc-ultra.o`	smc-ultra=*`io_port`*,*`IRQ`* *O* smc-ultra io=*`io_port`* irq=*`IRQ`*
Tarjeta Ethernet SMC Ultra32 EISA (32K)	`smc-ultra32.o`	

Hardware	Módulo	Parámetros
Sun BigMac Ethernet	`sunbmac.o`	
Sundance ST201 Alta	`sundance.o`	
Sun Happy Meal Ethernet	`sunhme.o`	
Sun Quad Ethernet	`sunqe.o`	
ThunderLAN	`tlan.o`	
Tarjetas Ethernet PCI Digital 21x4x Tulip SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	
Tarjetas Ethernet rápidas PCI VIA Rhine con VIA VT86c100A Rhine-II PCI o 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	
Tarjeta ISA AT&T GIS (nee NCR) WaveLan	`wavelan.o`	wavelan=*`[IRQ,0],io_port,NWID`*
Tarjetas Ethernet compatibles con WD8003 y WD8013	`wd.o`	wd=*`io_port`*,*`IRQ`*,*`mem`*,*`mem_end`* *OR* wd io=*`io_port`* irq=*`IRQ`* mem=*`mem`* mem_end=*`end`*
Compex RL100ATX-PCI	`winbond.o`	
Packet Engines Yellowfin	`yellowfin.o`	
Broadcom BCM5700 10/100/1000 ethernet adapter	`bcm5700`	
Intel Ether Express/100 driver	`e100`	
Shared-Memory IBM Token Ring 16/4	`ibmtr`	
IBM Olympic-based PCI token ring	`olympic`	
SIS 900/701G PCI Fast Ethernet	`sis900`	

Tabla A-5. Parámetros del módulo Ethernet

A continuación le ponemos algunos ejemplos de estos módulos:

Configuración	Ejemplo
Tarjeta ISA NE2000 en dirección ES 300 e IRQ 11	ne=0x300,11 ether=0x300,11,eth0
Tarjeta Wavelan en ES 390, autoprueba para IRQ y usando NWID para 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

Tabla A-6. Ejemplos de configuración de parámetros Ethernet

A.4.1. Utilización de múltiples tarjetas Ethernet

Puede usar más de una tarjeta Ethernet en una máquina. Si cada tarjeta utiliza un controlador diferente (por ejemplo, un 3c509 y un DE425), deberá sencillamente añadir `alias` (y posiblemente `opciones`) a cada una de las tarjetas en `/etc/conf.modules`. Consulte el *Manual oficial de personalización de Red Hat Linux* para obtener más información al respecto.

Si dos tarjetas Ethernet utilizan el mismo controlador (por ejemplo, dos 3c509 o una 3c595 y una 3c905), necesitará especificar en la línea de las opciones del controlador las direcciones de ambas tarjetas (en el caso de las tarjetas ISA) o (en el caso de las tarjetas PCI) deberá añadir una línea de `alias` para cada una de las tarjetas.

Para obtener información adicional sobre el uso de más de una tarjeta Ethernet, consulte *Linux Ethernet-HOWTO* en http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

Índice

Symbols

.fetchmailrc, 232
  opciones de usuario, 234
  opciones del servidor, 233
  opciones globales, 233
.procmailrc, 236
/etc/exports, 266
/etc/fstab, 268
/etc/named.conf
  (Ver BIND)
/etc/pam.conf, 119
  (Ver También PAM)
/etc/pam.d, 119
  (Ver También PAM)
/etc/sysconfig
  >/etc/sysconfig/amd, 68
  >/etc/sysconfig/apmd, 69
  >/etc/sysconfig/arpwatch, 69
  >/etc/sysconfig/authconfig, 69
  >/etc/sysconfig/clock, 69
  >/etc/sysconfig/desktop, 70
  >/etc/sysconfig/dhcpd, 70
  >/etc/sysconfig/hwconf, 71
  >/etc/sysconfig/identd, 71
  >/etc/sysconfig/init, 71
  >/etc/sysconfig/ipchains, 72
  >/etc/sysconfig/iptables, 72
  >/etc/sysconfig/rhn directory, 80
  /etc/sysconfig/irda, 73
  /etc/sysconfig/keyboard, 73
  /etc/sysconfig/kudzu, 74
  /etc/sysconfig/mouse, 74
  /etc/sysconfig/named, 75
  /etc/sysconfig/netdump, 75
  /etc/sysconfig/network, 76
  /etc/sysconfig/ntpd, 76
  /etc/sysconfig/pcmcia, 76
  /etc/sysconfig/radvd, 77
  /etc/sysconfig/rawdevices, 77
  /etc/sysconfig/redhat-config-users, 77
  /etc/sysconfig/samba, 78
  /etc/sysconfig/sendmail, 78
  /etc/sysconfig/soundcard, 78
  /etc/sysconfig/squid, 78
  /etc/sysconfig/tux, 78
  /etc/sysconfig/ups, 79
  /etc/sysconfig/vncservers, 79
  /etc/sysconfig/xinetd, 80
  directorio /etc/sysconfig network-scripts, 80
    (Ver También network)
  directorio /etc/sysconfig/apm-scripts/ directory, 80
  directorio /etc/sysconfig/cbq, 80
  directorio /etc/sysconfig/networking/, 80
/lib/security/, 119
  (Ver También PAM)
/proc
  recursos adicionales, 56
    documentación instalada, 56
    sitios web útiles, 57
/var/named/, 252
filtrado de paquetes
  (Ver iptables)
módulos de kernel
  módulos Ethernet
    ejemplos, 295
  tipos de, 285
módulos NIC
  (Ver módulos kernel)
protocolo SSH
  secuencia de conexión, 138

A

aboot, 64, 83
AccessFileName
  directiva de configuración de Apache, 208
Action
  directiva de configuración de Apache, 214
AddDescription
  directiva de configuración de Apache, 212
AddEncoding
  directiva de configuración de Apache, 213
AddHandler
  directiva de configuración de Apache, 213
AddIcon
  directiva de configuración de Apache, 212
AddIconByEncoding
  directiva de configuración de Apache, 212
AddIconByType
  directiva de configuración de Apache, 212
AddLanguage
  directiva de configuración de Apache, 213
AddType
  directiva de configuración de Apache, 213
Alias
  directiva de configuración de Apache, 210
Allow
  directiva de configuración de Apache, 207
AllowOverride
  directiva de configuración de Apache, 206
Apache
    (Ver Servidor HTTP de Apache)
  recursos adicionales, 221
    libros relacionados, 221
    sitios Web útiles, 221
apagado
  Servidor HTTP de Apache, 200

apagar, 80
arranque
  Servidor HTTP de Apache, 200
  servidor seguro, 200
arrastrar y soltar, xv
ataque Denial odf Service, 52
    (Ver También directorio /proc/sys/net/)
  definición de, 52
ataque DoS
  (Ver ataque Denial odf Service)
authconfig
  y LDAP, 280, 280
autofs, 268

B

Berkeley Internet Name Domain
  (Ver BIND)
BIND, 245
  >Recursos adicionales
    Sitios web útiles, 262
  Configuración
    >Registros de recursos de ficheros de zona, 253
    Directivas de los ficheros de zona, 252
    Ficheros de zona, 252
    Resolución de nombres inversa, 256
  Configuración de
    Ejemplos de ficheros de zona, 255
  demonio named, 247
  Ejemplos de declaraciones de zone , 251
  Errores frecuentes, 261
  Ficheros de configuracio´n, 247
  ficheros de configuración
    /etc/named.conf, 247
    directorio /var/named/, 247
  Introduccio´n, 245
  programa rndc, 257
    /etc/rndc.conf, 258
    configuración de claves, 258
  Propiedades
    IPv6, 261
    Mejoras del DNS, 260
    Seguridad, 260
    Visualizaciones múltiples, 260
  Propiedades avanzadas, 259
  Recursos adicionales, 261
    Documentación instalada, 261
    Libros, 262
  rndc
    configuración de named en uso , 257
    opciones de la línea de comandos, 258
  servidor de nombre
    definición de, 245
  servidor de nombre de root
    definición de, 245
  tipos de nombre de servidor
    solo caché, 246
  tipos de nombres de servidor
    posterior, 246
  Tipos de servidores de nombres
    esclavo, 246
    maestro, 246
  zonas
    definición de, 246
BIOS
  definición de, 59
    (Ver También proceso de arranque)
BrowserMatch
  directiva de configuración de Apache, 214

C

CacheNegotiatedDocs
  directiva de configuración de Apache, 208
carga directa
  carga de cadena, 83
chkconfig, 67
  (Ver También servicios)
configuración
  Apache, 201
  máquinas virtuales, 219
  SSL, 217
contraseña, 123
    (Ver También PAM)
  contraseñas shadow, 123
control del acceso
  (Ver wrappers TCP)
convenciones
  documento, xii
copiar y pegar un texto
  usando X, xv
correo electrónico, 223
  Fetchmail, 231
  Procmail, 235
  protocolos, 223
    IMAP, 223
    POP, 224
    SMTP, 225
  recursos adicionales, 242
    documentación instalada, 243
    libros relacionados, 244
    sitios Web útiles, 243
  seguridad, 241
    clientes, 241
    servidores, 242
  Sendmail, 227
  tipos, 226
    MDA (Mail Delivery Agent, Agente de entrega de correo), 226

MTA (Mail Transfer Agent, Agente de transferencia de correo, 226
MUA (Mail User Agent, Agente de usuario de correo), 226
CustomLog
directiva de configuración de Apache, 209

D

DefaultIcon
directiva de configuración de Apache, 212
DefaultType
directiva de configuración de Apache, 208
demonio named
(Ver BIND)
Denegación de servicio, 132
(Ver También xinetd)
Deny
directiva de configuración de Apache, 207
directivas de caché para Apache, 215
directivas de configuración directives, Apache
MaxRequestsPerChild, 203
directivas de configuración, Apache, 201
AccessFileName, 208
Action, 214
AddDescription, 212
AddEncoding, 213
AddHandler, 213
AddIcon, 212
AddIconByEncoding, 212
AddIconByType, 212
AddLanguage, 213
AddType, 213
Alias, 210
Allow, 207
AllowOverride, 206
BrowserMatch, 214
CacheNegotiatedDocs, 208
CustomLog, 209
DefaultIcon, 212
DefaultType, 208
deny, 207
Directory, 205
DirectoryIndex, 207
DocumentRoot, 205
ErrorDocument, 214
ErrorLog, 209
ExtendedStatus, 204
Group, 205
HeaderName, 212
HostnameLookups, 209
IfDefine, 204
IfModule, 208
Include, 203
IndexIgnore, 213
IndexOptions, 211
KeepAlive, 202
KeepAliveTimeout, 202
LanguagePriority, 213
Listen, 203
LoadModule, 204
Location, 215
LogFormat, 209
LogLevel, 209
MaxClients, 203
MaxKeepAliveRequests, 202
MaxSpareServers, 202
MetaDir, 214
MetaSuffix, 214
MinSpareServers, 202
NameVirtualHost, 216
Options, 206
Order, 207
para funcionalidad de caché, 215
para funcionalidad SSL, 217
PidFile, 201
ProxyRequests, 215
ProxyVia, 215
ReadmeName, 212
Redirect, 211
ScoreBoardFile, 201
ScriptAlias, 211
ServerAdmin, 205
ServerName, 205
ServerRoot, 201
ServerSignature, 210
SetEnvIf, 217
StartServers, 203
Timeout, 202
TypesConfig, 208
UseCanonicalName, 208
User, 204
UserDir, 207
VirtualHost, 216
directivas de configuracuión, Apache
LockFile, 201
directivas SSL, 217
directorio /etc/sysconfig, 24
directorio /etc/sysconfig/
(Ver directorio sysconfig)
directorio /lib, 20
directorio /mnt, 20
directorio /proc, 21
Directorio /sbin, 21
directorio /usr, 21
directorio /usr/local, 24
directorio /var/lib/rpm , 24
directorio /var/spool/up2date , 24
directorio initrd, 24
directorio sysconfig
/etc/sysconfig/network-scripts, 169

/etc/sysconfig/redhat-logviewer, 77
directorios en, 80
ficheros encontrados en, 67
información adicional sobre, 67
directorio/dev, 20
directorio/etc, 20
directorio/opt, 20
directorio/proc, 25
(Ver También sistema de ficheros /proc)
directorio/usr/local, 22
directorio/var directory, 22
directorios
/dev, 20
/etc, 20
/lib, 20
/mnt, 20
/opt, 20
/proc, 21
/sbin, 21
/usr, 21
/usr/local, 22, 24
/var, 22
directoriosysconfig
/etc/sysconfig/firstboot, 70
/etc/sysconfig/harddisks, 70
directoriosysconfig directory
/etc/sysconfig/gpm, 70
Directory
directiva de configuración de Apache, 205
DirectoryIndex
directiva de configuración de Apache, 207
dispositivo de frame buffer, 30
(Ver También /proc/fb)
dispositivos de bloque, 28
(Ver También /proc/devices)
definición de, 28
dispositivos de caracteres, 28
(Ver También /proc/devices)
definición de, 28
dispositivos, local
propiedad de, 125
(Ver También PAM)
DNS, 245
(Ver También BIND)
documentación
cómo encontrar, x
gurú, xii
usuario experimentado, xii
usuarios principiantes, x
libros, xii
sitios Web, xi
documentatión
usuarios principiantes
grupos de noticias, xi
DocumentRoot
cambiar, 219
cambiar las opciones compartidas, 219
directiva de configuración de Apache, 205
domnios de ejecución
definición de, 29
DoS
(Ver Denegación de servicio)
drivers
(Ver módulos de kernel)
DSOs
cargar, 218

E

El sistema X Window
(Ver XFree86)
ELILO, 64, 83
entornos de escritorio
(Ver XFree86)
Entrada y salida del sistema básica
(Ver BIOS)
ErrorDocument
directiva de configuración de Apache, 214
ErrorLog
directiva de configuración de Apache, 209
estructura
común, 19
Ethernet, 170
ExtendedStatus
directiva de configuración de Apache, 204

F

Fetchmail, 231
opciones de comando, 234
especiales, 235
informativas, 235
opciones de configuración, 232
opciones de usuario, 234
opciones del servidor, 233
opciones globales, 233
recursos adicionales, 242
FHS, 19, 20
(Ver También sistema de ficheros)
ficheros virtuales
(Ver sistema de ficheros proc)
ficheros, sistema de ficheros proc
cambiar, 26
visualización, 25, 56
formato común del fichero de logfile, 209
FrontPage, 200

G

gestores de arranque, 83, 91, 83
(Ver También aboot)
definición de , 83
tipos de, 83
Gestores de pantalla
(Ver XFree86)
gestores de ventanas
(Ver XFree86)
GNOME, 109
(Ver También XFree86)
GQ aplicación, 276
(Ver También LDAP)
Group
directiva de configuración de Apache, 205
groups
herramientas para la gestión de
redhat-config-users, 95
GRUB, 60
(Ver También gestores de arranque)
cambiar los niveles de ejecución con, 93
comandos, 88
definición de, 83
fichero de configuración
/boot/grub/grub.conf, 90
comandos, 89
fichero de configuración de menú, 89
estructura, 90
funciones, 84
instalación, 85
interfaces, 87
editor de entrada de menú, 87
línea de comandos, 87
menú, 87
orden de uso, 88
proceso de arranque, 83
recursos adicionales, 94
documentación instalada, 94
sitios Web útiles, 94
rol en el proceso de arranque, 60
terminología, 85
dispositivos, 85
ficheros, 86
sistema de ficheros raíz, 87
grub.conf, 90
(Ver También GRUB)
grupos, 95
definición de, 95
estándar, 97
GID, 95
herramientas de gestión de
groupadd, 99
herramientas para la gestión de
groupadd, 95
redhat-config-users, 99
privados de usuario
concepto, 100
privados de usuarios, 95
usuarios privados, 99
grupos de usuarios privados
(Ver grupos)
grupos privados de usuario
concepto, 100

H

halt, 80
HeaderName
directiva de configuración de Apache, 212
Herramienta de configuración de servicios, 67
(Ver También servicios)
HostnameLookups
directiva de configuración de Apache, 209
hosts.allow
(Ver wrappers TCP)
hosts.deny
(Ver wrappers TCP)
httpd.conf
(Ver directivas de configuración, Apache)

I

IfDefine
directiva de configuración de Apache, 204
ifdown, 174
IfModule
directiva de configuración de Apache, 208
ifup, 174
Include
directiva de configuración de Apache , 203
inclusión en el servidor, 206, 213
máquinas virtuales, 206
IndexIgnore
directiva de configuración de Apache, 213
IndexOptions
directiva de configuración de Apache, 211
init
rol en el proceso de arranque, 62
(Ver También proceso de arranque)
init command, 62
(Ver También proceso de arranque)
directorios usados por, 65
niveles de ejecución a los que se accede por, 66
SysV init
definición de, 65
interrupción
servidor seguro, 200
introducción, ix
ipchains
(Ver iptables)

iptables
>opciones de identificación de paquetes, 182
cadenas
destino, 177
comparado con ipchains, 178
guardar reglas, 186
lista de reglas, 177
opciones, 179
comandos, 180
estructura, 180
listado, 186
objetivo, 184
parámetros, 181
tablas, 179
opciones de selección
módulos, 184
protocolos
ICMP, 183
TCP, 182
UDP, 183
recursos adicionales, 187
documentación isntalada, 187
sitios web útiles, 187
reglas básicas del filtrado de paquetes, 177
tablas, 177
vista general de, 177

J

jerarquía, sistema de ficheros, 19

K

KDE, 109
(Ver También XFree86)
KeepAlive
directiva de configuración de Apache, 202
KeepAliveTimeout
directiva de configuración de Apache, 202
Kerberos
Centro de distribución de claves (KDC), 147
configuración de clientes , 150
configurar servidor , 148
definición de , 145
modo en que funciona, 147
razones para el uso, 145
razones para no usarlo, 145
recursos adicionales, 151
documentación instalada, 151
sitios Web útiles, 151
terminología, 146
Ticket Granting Service(TGS), 147
Ticket Granting Ticket (TGT), 147
y PAM, 148
kernel
rol en el proceso de arranque, 61

L

LanguagePriority
directiva de configuración de Apache, 213
LDAP
aplicaciones
GQ, 276
ldapadd, 274
ldapdelete, 274
ldapmodify, 274
ldapsearch, 274
paquete OpenLDAP, 274
slapadd, 274
slapcat, 274
slapd, 274
slapindex, 274
slappasswd, 274
slurpd, 274
utilidades, 274
applicaciones
slapcat-gdbm, 274
autenticación mediante, 280
PAM, 280
autenticación mediante el uso
authconfig, 280
configuración de clientes, 280
editing /etc/openldap/ldap.conf, 280
modificar /etc/nsswitch.conf, 280
autenticación mediante el uso de
modificar slapd.conf, 280
autenticación usando
paquetes, 280
authenticación mediante el uso
modificar /etc/ldap.conf, 280
características OpenLDAP, 273
configuración, 279
migración a los directorios 1.x, 279
definición de, 273
demonios, 274
ficheros de configuración
/etc/ldap.conf, 277
/etc/openldap/ldap.conf, 277
/etc/openldap/schema/ directorio, 278
/etc/openldap/schema/ directory, 277
/etc/openldap/slapd.conf, 277, 277
LDAPv2, 273
LDAPv3, 273
recursos adicionales, 281
documentación instalada, 282
libros relacionados, 282
sitios Web útiles, 282
terminología, 276
usar con NSS, 275

usar con PAM, 275
usar con PHP4, 275
usar con Servidor HTTP de Apache, 275
ventajas de, 273
ldapadd comando, 274
(Ver También LDAP)
ldapdelete comando, 274
(Ver También LDAP)
ldapmodify comando, 274
(Ver También LDAP)
ldapsearch comando, 274
(Ver También LDAP)
LILO, 60
(Ver También gestores de arranque)
cambiar los niveles de ejecución con, 93
definición de, 91
fichero de configuración
/etc/lilo.conf, 92
proceso de arranque, 91
recursos adicionales, 94
documentación instalada, 94
sitios Web útiles, 94
rol en el proceso de arranque, 60
lilo.conf, 92
(Ver También LILO)
Listen
directiva de configuración de Apache, 203
llave de petición del sistema
definición de , 47
habilitar, 47
LoadModule
directiva de configuración de Apache, 204
Location
directiva de configuración de Apache, 215
LockFile
directiva de configuración de Apache, 201
log files
formato común del fichero de log, 209
LogFormat
directiva de configuración de Apache, 209
LogLevel
directiva de configuración de Apache, 209

M

Master Boot Record
(Ver MBR)
(Ver MBR)
MaxClients
directiva de configuración de Apache, 203
MaxKeepAliveRequests
directiva de configuración de Apache, 202
MaxRequestsPerChild
directiva de configuración de Apache, 203
MaxSpareServers
directiva de configuración de Apache, 202
MBR
definición de, 59, 59
(Ver También gestor de arranque)
MDA
(Ver Mail Delivery Agent, Agente de entrega de correo)
MDA (Mail Delivery Agent, Agente de entrega de correo), 226
Metacity
(Ver XFree86)
MetaDir
directiva de configuración de Apache, 214
MetaSuffix
directiva de configuración de Apache, 214
MinSpareServers
directiva de configuración de Apache, 202
MTA
(Ver Mail Transfer Agent, Agente de transferencia de correo)
MTA (Mail Transfer Agent, Agente de transferencia de correo), 226
MUA
(Ver Mail User Agent, Agente de usuario de correo)
MUA (Mail User Agent, Agente de usuario de correo), 226
máquina virtual
Listen command, 220
máquinas virtuales
basadas en el nombre, 219
configurar, 219
inclusión en el servidor, 206, 213
Options, 206
módulos
(Ver módulos de kernel)
(Ver módulos de kernel)
Apache
cargar, 218
sus , 218
predeterminados, 217
Módulos de autenticación conectables (PAM)
(Ver PAM)
módulos de CD-ROM
(Ver módulos de kernel)
módulos de kernel
introducción, 285
módulos de CD-ROM
ejemplos, 287
parámetros, 286
módulos Ethernet
parámetros, 292
soporte de múltiples tarjetas, 296
módulos SCSI
ejemplos, 291
parámetros, 288

parámetros de módulo
especificar, 285
módulos Ethernet
(Ver módulos de kernel)
módulos SCSI
(Ver módulos de kernel)
módulos Servidor HTTP de Apache, 217

N

NameVirtualHost
directiva de configuración de Apache, 216
netfilter
(Ver iptables)
Network File System
(Ver NFS)
NFS
cliente
/etc/fstab, 268
autofs, 268
configuración, 267
opciones de montaje, 269
introducción, 263
metodología, 263
portmap, 264
recursos adicionales, 271
documentación instalada, 271
libros relacionados, 271
seguridad, 270
acceso al sistema, 270
permisos de ficheros, 271
servidor
ficheros de configuración, 265
niveles de ejecución, 66
cambiar el tiempo de arranque, 93
ntsysv, 67
(Ver También servicios)

O

objetos dinámicamente compartidos
(Ver DSOs)
OpenLDAP
(Ver LDAP)
OpenSSH
ficheros de configuración, 140
opinión
información de contacto, xvi
Options
directiva de configuración de Apache, 206
Order
directiva de configuración de Apache, 207

P

PAM
contraseñas shadow, 123
definición de , 119
ficheros de configuración, 119
indicadores de control, 121
muestras de configuración, 122
módulos, 120
apilar, 120, 122
argumentos, 122
componentes, 120
creación, 121
localización de , 122
tipos, 120
nombres de servicio, 119
otros recursos
sitios web útiles, 126
pam_console
definición de , 125
recursos adicionales, 125
documentación instalada, 125
ventajas de, 119
y Kerberos, 148
pam_console
(Ver PAM)
parámetros de módulo
(Ver módulos de kernel)
PidFile
directiva de configuración de Apache, 201
portmap, 264
rpcinfo, 264
prefdm
(Ver XFree86)
proceso de arranque, 59, 59
carga directa, 83
etapas
BIOS, 59
etapas de, 59, 59
comando /sbin/init, 62
gestor de arranque, 60
kernel, 61
Shell EFI, 59
para x86, 59
Procmail, 235
configuración, 236
recetas, 237
acciones especiales, 239
condiciones especiales, 239
ejemplos, 240
entrega, 238
indicadores, 238
lockfile local, 239
no entrega, 238
recursos adicionales, 242
programas

ejecución en tiempo de arranque, 64
protocolo SSH
autenticación, 140
capas de, 138
canales, 140
ficheros de configuración, 140
protocolos inseguros y, 143
reenvío del puerto, 142
reenvío por TCP/IP, 141
reenvío por X11, 142
requisitos para la conexión remota, 143
Sesiones X11, 141
ProxyRequests
directiva de configuración de Apache, 215
ProxyVia
directiva de configuración de Apache, 215
public_html directories, 207

R

ratón
cómo utilizarlo, xv
rc.local
modificar, 64
ReadmeName
directiva de configuración de Apache, 212
red
comandos
/sbin/ifdown, 174
/sbin/ifup, 174
/sbin/service network, 174
configuración, 170
funciones, 175
interfaces, 170
acceso telefónico, 171
alias, 173
clon, 173
Ethernet, 170
recursos adicionales, 175
scripts, 169
Redirect
directiva de configuración de Apache, 211
rpcinfo, 264

S

sawfish, 109
(Ver También XFree86)
ScoreBoardFile
directiva de configuración de Apache, 201
ScriptAlias
directiva de configuración de Apache, 211
scripts CGI
fuera de ScriptAlias, 213
permitir ejecuciones externas cgi-bin, 206
seguridad
configuración, 217
ejecutar Apache sin, 219
Sendmail, 227
alias, 229
cambios de configuración comunes, 229
con UUCP, 229
correo basura, 230
historia, 227
instalación por defecto, 228
LDAP y, 231
limitaciones, 227
máscaras, 229
objetivo, 227
recursos adicionales, 242
ServerAdmin
directiva de configuración de Apache, 205
ServerName
directiva de configuración de Apache, 205
ServerRoot
directiva de configuración de Apache, 201
ServerSignature
directiva de configuración de Apache, 210
servicios
configuración con Herramienta de configuración de servicios, 67
configuración conchkconfig, 67
configuración conntsysv, 67
servidor de nombre
(Ver BIND)
servidor de nombre de root
(Ver BIND)
servidor de nombre de sólo caché
(Ver BIND)
servidor de nombre esclavo
(Ver BIND)
servidor de nombre maestro
(Ver BIND)
servidor de nombre posterior
(Ver BIND)
Servidor HTTP de Apache
apagado, 200
arranque, 200
configuración, 201
ejecutar sin seguridad, 219
ficheros log, 201
informes sobre el estado del servidor, 215
introducción, 189
reanudar, 200
recargar, 200
resolución de problemas, 201
versión 1.3
migración a la versión 2.0, 191
versión 2.0
cambios en el sistema de ficheros, 190
cambios en los paquetes, 190

características de, 189
migración desde la versión 1.3, 191
servidor no seguro
desactivar, 219
servidor proxy, 215, 215
servidor seguro
apagado, 200
arranque, 200
reanudar, 200
SetEnvIf
directiva de configuración de Apache, 217
shadow
(Ver contraseñas)
utilidades, 100
Shell de interfaz Firmware extensible
(Ver Shell EFI)
Shell EFI
definición de, 59
sistema
apagar, 80
sistema de ficheros
estructura, 19
estándar FHS, 20
jerarquía, 19
organización, 20
virtual
(Ver sistema de ficheros proc)
sistema de ficheros /proc, 25
/proc/apm, 27
/proc/cmdline, 27
/proc/cpuinfo, 28
/proc/dma, 29
/proc/fb, 30
/proc/file systems, 30
/proc/interrupts, 30
/proc/iomem, 31
/proc/ioports, 32
/proc/isapnp, 32
/proc/kcore, 33
/proc/kmsg, 33
/proc/ksyms, 33
/proc/loadavg, 34
/proc/mdstat, 34
/proc/meminfo, 35
/proc/misc, 36
/proc/modules, 36
/proc/mtrr, 37
/proc/partitions, 37
/proc/slabinfo, 38
/proc/stat, 39
devices
dispositivos de bloque, 28
directorio /proc/ide/, 43
execdomains, 29
ficheros en, alto nivel, 26
visualización de ficheros, 25
sistema de ficheros proc
>directorio /proc/tty , 55
>directorio/proc/sys/, 47
/proc/devices
dispositivos de caracteres, 28
/proc/swaps, 39
/proc/version, 40
cambiar ficheros en , 26, 56
directorio /proc/driver/, 43
directorio /proc/ide/ directory
directorios de dispositivo, 44
directorio /proc/sys/, 56
(Ver También sysctl)
/proc/sys/kernel/sysrq
(Ver llave de petición del sistema)
directorio /proc/sys/net/, 52
directorio/proc/ys/vm/, 54
directorio /proc/sysvipc/, 55
directorio/proc/irq/, 45
directorio/proc/net/, 45
directorio/proc/scsi/, 46
directorio/proc/sys/
directorio/proc/sys/fs/, 49
directorios de proceso, 40
directorioself, 42
subdirectorios en, 40
sistema de ficheros virtual
(Ver sistema de ficheros proc)
sistema de ficheros/proc
/proc/mounts, 36
/proc/pci, 37
sistema de ficherosproc
>directorio /proc/sys/
directorio /proc/sys/kernel/, 50
cambiar ficheros en, 47
directorio/proc/sys/
directorio/proc/sys/dev/, 49
sistema de focheros proc
directorio /proc/bus/, 42
sisteme de ficheros proc
/proc/uptime, 39
sitema de ficheros /proc
/proc/locks, 34
slapadd comando, 274
(Ver También LDAP)
slapcat comando, 274
(Ver También LDAP)
slapcat-gdbm command, 274
(Ver También LDAP)
slapd comando, 274
(Ver También LDAP)
slapindex comando, 274
(Ver También LDAP)
slappasswd comando, 274
(Ver También LDAP)
slurpd comando, 274

(Ver También LDAP)
SSH, 137
capas, 138
introducción, 137
protocolo
capa de transporte, 139
riesgos de la seguridad, 138
StartServers
directiva de configuración de Apache, 203
startx, 110
(Ver También XFree86)
stunnel, 242
sysconfig directorio
/etc/sysconfig/iptables, 186
sysctl
configurar con /etc/sysctl.conf, 56
controlar /proc/sys/, 56
SysReq
(Ver llave de petición del sistema)
SysRq
(Ver llave de petición del sistema)
SysV init
(Ver init command)

T

Timeout
directiva de configuración de Apache, 202
Tripwire
aplicaciones, 163
tripwire, 163
twadmin, 161, 163, 163
twinstall.sh, 163
twprint, 158, 159, 163
base de datos
actualización, 161
definición de, 164
inicialización de, 158
control de integridad
comando tripwire --check, 158
fichero de política
actualización, 161
modicación, 156
ficheros de configuración, 163
actualización, 163
fichero de la base de datos, 163, 164
ficheros clave, 163
ficheros de informe, 163, 164
firma de, 163
modificación, 155
tw.cfg, 163, 164
tw.pol, 163, 164
twcfg.txt, 163
twpol.txt, 163
funciones de correo electrónico, 162
pruebas, 163
informes
definición de, 164
visualización, 158
instalación de
comando tripwire --init , 158
configuración de contraseñas, 157
inicialización de la base de datos de Tripwire, 158
instalación de RPM, 154
personalizar la configuración, 155
script twinstall.sh, 157
introducción, 153
otros recursos, 165
documentación instalada, 165
sitios web útiles, 165
uso de, 153
TypesConfig
directiva de configuración de Apache, 208

U

ubicación de los ficheros de Red Hat Linux
/etc/sysconfig/, 24
(Ver También /etc/sysconfig)
/var/lib/rpm, 24
/var/spool/up2date/, 24
UseCanonicalName
directiva de configuración de Apache, 208
User
directiva de configuración de Apache, 204
UserDir
directiva de configuración de Apache, 207
users
directorios HTML personales, 207
usuarios, 95
/etc/passwd, 95
estádar, 95
herramientas para la gestión de
redhat-config-users, 95
useradd, 95
tipos de, 95
UID, 95
utilidad APXS Apache, 218
utilidades
shadow, 100
utilidades de initscript, 67
(Ver También servicios)

V

VirtualHost
directiva de configuración de Apache, 216

W

webmaster
  dirección de e-mail para, 205
Windowmaker
  (Ver wmaker)
wmaker, 109
  (Ver También XFree86)
wrappers TCP
  control de acceso
    características, 128
    comodines, 128
    regla para formatear, 128
  control del acceso, 127
    /etc/hosts.allow, 127
    /etc/hosts.deny, 127
    comandos de la shell , 130
    expansiones, 130
    operadores, 129
  definición de, 127
  recursos adicionales, 135
    documentación adicional, 135
    sitios web útiles, 136
  usos para, 127
  ventajas de, 127
  xinetd, 131

X

X
  (Ver XFree86)
X.500
  (Ver LDAP)
X.500 Lite
  (Ver LDAP)
XFree86
  clientes X, 103
    comandoxinit, 108
    entornos de escritorio, 109
    gestores de ventanas, 108, 109
    GNOME, 109
    KDE, 109
    mwm (Metacity), 109
    sawfish, 109
    twm, 109
    wmaker, 109
  entornos de escritorio, 109
  ficheros de configuración
    /etc/X11/ directory, 105
    /etc/X11/XF86Config, 105
    opciones dentro de, 105
  fuentes, 112
  Gestores de pantalla X
    definición de, 111
    gdm, 111
    kdm, 111
    prefdm script, 111
    xdm, 111
  introducción, 103
  niveles de ejecución, 110
    3, 110
    5, 111
  recursos adicionales, 114
    documentación instalada, 114
    libros relacionados, 114
    sitios web útiles, 114
  servidor de fuente X
    añadir fuentes, 113
    configuración de, 112
    xfs, 112
  servidor fuente X
    xfs, 105
  servidor X, 103
    características de, 104
    XFree86, 104
  utilidades
    Herramienta de configuración de X, 103
xfs
  (Ver XFree86)
xinetd, 131
    (Ver También wrappers TCP)
  >desvío del puerto, 134
  control del acceso con, 133
  ficheros de configuración, 131
    /etc/xinetd.conf, 131
    directorio/etc/xinetd.d/, 132
  para prevenir ataques de DoS, 132
  vinculación, 134
xinetd.conf
  (Ver xinetd)
xinit
  (Ver XFree86)

Colophon

Los manuales oficiales de Red Hat Linux manuals están escritos en formato DocBook SGML v4.1. Los formatos HTML y PDF se producen mediante el uso de la hojas de estilo DSSSL y scripts personalizados de wrappers jade.

Marianne Pecci <goddess@ipass.net> es la creadora de las imágenes de advertencia (nota, sugerencia, atención y aviso). Su redistribución es posible trámite un permiso por escrito firmado por Marianne Pecci y Red Hat, Inc..

El Equipo de Documentación del Producto Red Hat Linux está formado por las siguientes personas:

Sandra A. Moore — Escritora inicial y de las modificaciones del *Manual oficial de instalación de Red Hat Linux para x86*; Colaboradora en la escritura del *Manual oficial del principiante de Red Hat Linux*

Tammy Fox — Escritora inicial y de modificaciones del *Manual oficial de personalización de Red Hat Linux*; Colaboradora en la escritura del *Manual oficial del principiante de Red Hat Linux*; Escritora inicial y de modificaciones de las hojas de estilo personalizadas DocBook y los scripts

Edward C. Bailey — Colaborador en la escritura del *Manual oficial de instalación de Red Hat Linux para x86*

Johnray Fuller — Escritor inicial y de modificaciones del *Manual oficial de referencia de Red Hat Linux*; Colaborador en la escritura y modificación del *Manual oficial de seguridad de Red Hat Linux*

John Ha — Escritor inicial y de modificaciones del *Manual oficial del principiante de Red Hat Linux*; Colaborador en la escritura y modificaciones del *Manual oficial de seguridad de Red Hat Linux*